-5/7


# THE JOURNAL
## OF THE
# INDIAN MATHEMATICAL SOCIETY

NEW SERIES

*Vol. III* *No. 2* *June 1938*


OFFICE OF THE ... 28 OCT 1938 MADRAS

CONTENTS


E. T. Bell: Notes on Denumerants .. 41

Brij Mohan and R. V. Shastry: An Inversion Formula.. 46

R. Vaidyanathaswamy and T. Venkatarayudu: Canonical Basis for Ideals in a Polynomial Domain over a commutative Ring with finite basis for Ideals .. 49

R. S. Varma: On Laguerre Polynomials which are Self-reciprocal in the Hankel Transform .. 54

K. S. Suryanarayanan: On three Rational Functions on a Riemann Surface .. 56

Ram Behari: Infinitesimal Deformation of Ruled Surfaces .. 68

T. Venkatarayudu: The Algebra of the *e*th power Residues .. 73



MADRAS:

PRINTED AT THE MADRAS LAW JOURNAL PRESS, MYLAPORE

# THE JOURNAL
## OF THE
# INDIAN MATHEMATICAL SOCIETY

## NEW SERIES



*Editor*:
R. VAIDYANATHASWAMY, M.A., D.SC.

*Joint Editor*:
C. N. SRINIVASIENGAR, D. SC.

*Collaborators*:

K. ANANDA RAO, M.A.
S. C. DHAR, D. SC.
H. RAFAEL, D. SC., S.J.
S. R. U. SAVOOR. M.A., D.SC.
M. R. SIDDIQI, M.A., PH. D.
T. SURYANARAYANA, M.A.


THE JOURNAL OF THE INDIAN MATHEMATICAL SOCIETY (NEW SERIES) is a quarterly published at the end of March, June, September and December at a price of Re. 1-8-0 or 2*s*. 6*d*. for a single issue, or an Annual Subscription of Rs. 6-0-0 or 10*s*. for four issues.

Papers are invited on subjects of Pure and Applied Mathematics and should be addressed to **C. N. Srinivasiengar, D.Sc., Central College, Bangalore.** Authors of papers are entitled to 50 free reprints. If more copies are required they are supplied at net cost if previous intimation is given. Enquiries from persons desiring to become subscribers should be adressed to S. MAHADEVAN, M.A., L.T., Department of Mathematics, Presidency College, Madras.

OFFICE OF THE REGISTRAR OF BOOKS
28 OCT 1938
MADRAS

# NOTES ON DENUMERANTS

*By* E. T. BELL, *California.*

[Received 27 February 1938]

**1.** *A Characteristic Equation.* If $n, a_1, \dots, a_r$ are given integers, $n \geqslant 0, a_1 > 0, \dots, a_r > 0$, the number of sets $(x_1, \dots, x_r)$ of integers $x_1 \geqslant 0, \dots, x_r \geqslant 0$ such that

$$a_1 x_1 + \dots + a_r x_r = n$$

is (in Sylvester's terminology) the denumerant $A(n; a_1, \dots, a_r)$, or simply $A(n)$. If $x$ is not an integer $\geqslant 0$, $A(x)$ is defined to be zero. Let $e(0) = 1$, $e(x) = 0$, $x \neq 0$; and let $\sum_p$ refer to all selections of $p$ distinct members of the set $a_1, \dots, a_r$. Thus

$$\sum\nolimits_2 F(n - a_i - a_j)$$

refers to the $r(r-1)/2$ pairs $a_1, a_2; \dots; a_1, a_r; \dots; a_{r-1}, a_r$; etc.

Let $F(x) = 0$ if $x$ is not an integer $\geqslant 0$, and let $F(x)$ take integer values $> 0$ for integer values $\geqslant 0$ of $x$. We shall show that $F(x) = A(x)$ is the unique solution of

$$F(x) - \sum\nolimits_1 F(x - a_i) + \sum\nolimits_2 F(x - a_i - a_j)$$
$$- \sum\nolimits_3 F(x - a_i - a_j - a_k) + \dots + (-1)^r F(x - a_1 - \dots - a_r) = e(x). \tag{1.1}$$

If $x$ is not an integer $\geqslant 0$, (1.1) is identically satisfied, and $F(x) = A(x)$ is a solution. We therefore need consider only

$$F(n) - \sum\nolimits_1 F(n - a_i) + \dots = e(n), \tag{1.2}$$

with $n$ an integer $> 0$, as before.

From the generating identity

$$\prod_{i=1}^{r} (1 - y^{a_i})^{-1} = \sum_{n=0}^{\infty} A(n) y^n, \quad |y| < 1,$$

we have

$$1 = \prod_{i=1}^{r} (1 - y^{a_i}) \sum_{n=0}^{\infty} A(n) y^n.$$



129108

Hence

$$\sum_{n=1}^{\infty} e(n)y^n = \left(1-\sum_1 y^{a_i}+\sum_2 y^{a_i+a_j}-\ldots\right)\sum_{n=0}^{\infty} A(n)y^n,$$

$$= \sum_{n=0}^{\infty}\left[A(n)-\sum_1 A(n-a_i)+\ldots\right]y^n.$$

From the reversibility of the steps, and the uniqueness of the power series expansion of an analytic function (of $y$, here), the proposition follows.

2. *Determinant for* $A(n)$. Determinant expressions for $A(n)$ have been given by E. Fergola and C. Sardi.* A much simpler form is given at once by (1.2). We denote by $\phi_a(n)$, or simply $\phi(n)$, where $a = a_1+\ldots+a_r$, the number of partitions of $n$ into an even number of distinct parts chosen from $a_1,\ldots, a_r$, minus the like for an odd number of distinct parts, for $0 \leqslant n \leqslant a$. By convention, $\phi(0) = 1$; and if $n$ does not lie in the interval indicated, $\phi(n) = 0$. Then

$$\prod_{i=1}^{r}(1-y^{a_i}) = \sum_{n=0}^{\infty}\phi(n)y^n;$$

$$\sum_{n=0}^{\infty} e(n)y^n = \sum_{n=0}^{\infty}\phi(n)y^n \sum_{n=0}^{\infty} A(n)y^n;$$

$$e(n) = \phi(0)A(n)+\phi(1)A(n-1)+\ldots+\phi(n)A(0).$$

Replacing $n$ by $n, n-1,\ldots, 0$ in the last, and solving the resulting system of equations, we find, for $n > 0$,

$$A(n)=(-1)^n\begin{vmatrix} \phi(1) & \phi(2) & \phi(3) & \ldots & \phi(n-1) & \phi(n) \\ 1 & \phi(1) & \phi(2) & \ldots & \phi(n-2) & \phi(n-1) \\ 0 & 1 & \phi(1) & \ldots & \phi(n-3) & \phi(n-2) \\ 0 & 0 & 1 & \ldots & \phi(n-4) & \phi(n-3) \\ & \ldots & & & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & \phi(1) \end{vmatrix}.$$

As an example, for $r=2$ and $a_1=2$, $a_2=3$, $n=5$, we have $\phi(0)=1$, $\phi(2)=-1$, $\phi(3)=-1$, $\phi(5)=1$, and the determinant gives $A(5)=1$, which is correct, since $2x+3y=5$ has only the solution $(x, y)=(1, 1)$. For the same $a_1, a_2$ we get $A(6)=2$, correct, since $2x+3y=6$ has only the solutions $(x, y)=(3, 0)$, $(0, 2)$.

* *Giornale di Matematiche*, 1 (1863), 63-64; *ibid.* 3 (1865), 94-99, 377-380. See also Dickson's *History*, 2, 125.

**3.** *Reciprocity.* Consider the two sets of integers $a_1, \ldots, a_r > 0$, $b_1, \ldots, b_s > 0$, and the associated denumerants $A(n)$, $B(n)$. For the first set we have defined $\phi_a(n)$; for the second set we define $\phi_b(n)$ similarly. Between the denumerants $A, B$ there is a simple reciprocity:

$$\begin{vmatrix} A(n) & \phi_b(1) & \phi_b(2) & \cdot\cdot & \phi_b(n) \\ A(n-1) & \phi_b(0) & \phi_b(1) & \cdot\cdot & \phi_b(n-1) \\ A(n-2) & 0 & \phi_b(0) & \cdot\cdot & \phi_b(n-2) \\ & \cdot\cdot & \cdot\cdot & \cdot\cdot & \\ A(0) & 0 & 0 & & \phi_b(0) \end{vmatrix}$$

is equal to the determinant obtained from this when $A$ is replaced by $B$, and $b$ by $a$.

To prove this, let $r+s=t$, and let $c_1, \ldots, c_t$ be the set composed of $a_1, \ldots, a_r$, $b_1, \ldots, b_s$ in any order. Let $C(n)$ be the denumerant for $c_1, \ldots, c_t$, and $\phi_c(n)$ the function defined similarly to $\phi_a(n)$, $\phi_b(n)$. Then, for $|y| < 1$,

$$\prod_{i=1}^{r} (1-y^{a_i})^{-1} = \sum_{n=0}^{\infty} A(n) y^n, \quad \prod_{i=1}^{s} (1-y^{b_i})^{-1} = \sum_{n=0}^{\infty} B(n) y^n,$$

$$\prod_{i=1}^{t} (1-y^{c_i})^{-1} = \prod_{i=1}^{r} (1-y^{a_i})^{-1} \cdot \prod_{i=1}^{s} (1-y^{b_i})^{-1} = \sum_{n=0}^{\infty} C(n) y^n.$$

Multiplying the last by $\prod_{i=1}^{s} (1-y^{b_i})$, also by $\prod_{i=1}^{r} (1-y^{a_i})$, and equating coefficients of $y^n$ in the results, we get

$$C(n) + \phi_a(1) C(n-1) + \ldots + \phi_a(n) C(0) = B(n),$$
$$C(n) + \phi_b(1) C(n-1) + \ldots + \phi_b(n) C(0) = A(n).$$

Replacing $n$ by $n, n-1, \ldots, 0$ in each of these and solving the resulting systems for $C(n)$ we get two determinants for $C(n)$. The necessary equality of these is the reciprocity in question.

**4.** *Certain partition sums.* Let $\Sigma$ refer to all sets of integer solutions $(i_1, i_2, \ldots, i_n)$ of

$$i_1 + 2i_2 + 3i_3 + \ldots + n\, i_n = n,$$

$i_1 \geqslant 0, \ldots, i_n \geqslant 0$. Jacobi* gave a purely combinatorial proof of

$$\sum \frac{1}{1^{i_1} 2^{i_2} \ldots n^{i_n} \cdot i_1!\, i_2! \ldots i_n!} = 1, \tag{4.1}$$

* *Journal für Mathematik*, 22 (1841), 372-4. The same result was stated by several later writers, including Sylvester (1861) and Catalan (1886). Cauchy (*Oeuvres*, t. VI, p. 113), in 1841, gave similar results.

OFFICE OF THE ... 29 OCT 1938 MADRAS
600 008.

which seems to have been first noted as a consequence of equating coefficients in the identity

$$(1-y)^{-1} = e^{-\log(1-y)} = e^{y}e^{y^2/2}e^{y^3/3}\ldots, \quad |y| < 1.$$

Without attempting combinatorial proofs we note a more general result, (4.4) below, of a similar kind. For $y$, $x$ suitably restricted to secure absolute convergence, we have

$$(1-y)^{-x} = e^{xy/1}\,e^{xy^2/2}\,e^{xy^3/3}\ldots,$$

and hence, on comparing coefficients of $y^n$,

$$\sum \frac{x^{i_1+i_2+\ldots+i_n}}{1^{i_1}.2^{i_2}\ldots n^{i_n}.\,i_1!\,i_2!\ldots i_n!} = x(x+1)\ldots(x+n-1)/n!. \quad (4.2)$$

For $x = 1$, this gives (4.1). If in the derivative of (4.2) with respect to $x$ we put $x = 1$, we get

$$\sum \frac{i_1+\ldots+i_n}{1^{i_1}\ldots n^{i_n}.\,i_1!\ldots i_n!} = 1+\tfrac{1}{2}+\tfrac{1}{3}+\ldots+\tfrac{1}{n}. \quad (4.3)$$

Let $(n, r)$ denote the sum of all products $r$ at a time of distinct integers chosen from $1, 2, \ldots, n$, and let $(n, 0)=1$. Then

$$(x+1)(x+2)\ldots(x+n) = x^n + (n, 1)x^{n-1} + \ldots + (n, n).$$

If $P(x, y)$ is any polynomial in $x$, $y$, we have

$$\sum \frac{P(i_1+\ldots+i_n, y)}{1^{i_1}.2^{i_2}\ldots n^{i_n}.\,i_1!\,i_2!\ldots i_n!} = \frac{1}{n!}\sum_{t=0}^{n-1}(n-1, t)P(n-t, y). \quad (4.4)$$

This follows from (4.2). Replace $x$ by $e^x$ in (4.2) and equate coefficients of $x^s$ in the expanded result. Then, if $s$ is an integer $\geqslant 0$,

$$\sum \frac{(i_1+\ldots+i_n)^s}{1^{i_1}\ldots n^{i_n}.\,i_1!\ldots i_n!} = \frac{1}{n!}\sum_{t=0}^{n-1}(n-1, t)(n-t)^s. \quad (4.5)$$

If now $P(x, y) = p_0x^h + p_1x^{h-1}y + \ldots$, we replace $s$ by $h$ in (4.5) and multiply by $p_0$, then replace $s$ by $h-1$ and multiply by $p_1y$, and so on. Adding all the results we find (4.4). Conversely, for $y = 0$, $h = s$, (4.4) gives (4.5). For $s = 0$, (4.5) gives (4.1). Thus (4.4) includes all the results in this section.

5. *Connection with recurring series.* By successive applications of the operator $xd/dx$ to $x/(1-x)$ we sum the series

$\sum_{r=1}^{\infty} r^s x^r$. Thus for $s = 4$,

$$\sum_{r=0}^{\infty} r^4 x^r = \frac{x(1+11x+11x^2+x^3)}{(1-x)^5}, \quad |x| < 1. \tag{5.1}$$

Generally ($s$ an integer $> 0$), the sum is a rational function of the form $xQ_s(x)/(1-x)^{s+1}$, where $Q_s(x)$ is a reciprocal polynomial in $x$ of degree $s-1$ with integer coefficients, the coefficients of the highest and lowest powers of $x$ being each 1. Resolving $Q_4(x)$ into its linear factors, we have

$$1+11x+11x^2+x^3 = (1+x)(1+\alpha x)(1+\beta x);$$

here $\alpha = 5+2\sqrt{6}$, $\beta = 5-2\sqrt{6}$, but the actual form of the roots of $Q_s(x) = 0$ in any case is not needed. Hence

$$\sum_{r=1}^{\infty} r^4 x^r = e^{\log(1+x)+\log(1+\alpha x)+\log(1+\beta x)-5\log(1-x)}.$$

Expanding the logs in the exponent, we get

$$\sum_{n=1}^{\infty} \frac{x^n}{n}\,[5-(-1)^n+(-1)^{n-1}(\alpha^n+\beta^n)].$$

It is easily seen that the expression in square brackets is the solution $w_n$ of the difference equation

$$w_{n+2}+10w_{n+1}+w_n = 4[15+2(-1)^n],$$

which is defined by the initial values $w_0 = 2$, $w_1 = 16$. With $\sum$ as in § **4**, we have

$$\sum \frac{w_1^{i_1} w_2^{i_2} \ldots w_n^{i_n}}{1^{i_1} 2^{i_2} \ldots n^{i_n}.\, i_1!\, i_2! \ldots i_n!} = (n+1)^4.$$

In the same way, if $v_{n+2}-pv_{n+1}+qv_n = 0$, $v_0 = 2$, $v_1 = p$, we find

$$\sum \frac{(-1)^{i_1+i_2+\ldots+i_n} v_1^{i_1} v_2^{i_2} \ldots v_n^{i_n}}{1^{i_1}.\, 2^{i_2}.\, \ldots n^{i_n}.\, i_1!\, i_2! \ldots i_n!} = 0, \quad n \geqslant 2.$$

# AN INVERSION FORMULA

*By* BRIJ MOHAN *and* R. V. SHASTRY, *Benares University.*

[Received 10 December 1937]

**1.** Bateman* has proved that the inversion formula

$$\int_s^{\infty}\int_{-\infty}^{\infty} J_0(x-s)\frac{J_1(x-t)}{x-t}f(t)\,dt\,dx = 2f(s)$$

holds for a certain class of functions $f(x)$. This formula has been generalized by Hardy† who has obtained one containing Bessel functions of orders $\nu$ and $1-\nu$. Fox‡ has obtained the following result on somewhat different lines:

THEOREM A. *If $f(s)$ be defined by either of the formulae*

$$f(s) = \int_a^b \phi(\mu) \begin{matrix}\cos\\ \sin\end{matrix} \mu s\, d\mu,$$

*where*

$$\int_a^b |\phi(\mu)|\, d\mu$$

*exists, and $-1<a<b$, then*

$$\int_s^{\infty}\int_{-\infty}^{\infty}\left[\left\{(\nu-1)\frac{J_{\nu-1}(x-t)}{x-t}J_\nu(x-s)+\nu\frac{J_\nu(x-t)}{x-t}J_{\nu-1}(x-s)\right\}\times f(t)\,dt\right]dx = 2f(s), \qquad (1)$$

*where $\nu$ is an integer or zero.*

1.1. Fox has further shown in the same paper, that (1) holds for functions satisfying the relation

$$f(s) = \frac{1}{\pi}\int_{-\infty}^{\infty}\frac{\sin(s-t)}{s-t}f(t)\,dt.$$

1.2. Brij Mohan§ has further generalized the formula in the following

THEOREM B. *If $f(s)$ be defined by either of the formulae*

$$f(s) = \int_a^b \phi(\mu) \begin{matrix}\cos\\ \sin\end{matrix} \mu s\, d\mu,$$

* The inversion of a definite Integral, *Proc. Lond. Math. Soc.* (2), 4 (1906), 484.

† An integral equation, *Ibid.* (2), 7 (1909), 445-72.

‡ A generalization of an integral equation due to Bateman, *Ibid.* (2), 26 (1927), 395-402.

§ Some inversion formulae, *Proc. Benares Math. Soc.* 15 (1933), 1-20.

or
$$f(s) = \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{\sin(s-t)}{s-t} f(t)\, dt,$$
then
$$\int_s^{\infty} dx \int_{-\infty}^{\infty} \{ J_{\lambda+1}(x-s)J_{\lambda-1}(x-t) + J_\lambda(x-s)J_\lambda(x-t)$$
$$+ J_\nu(x-s)J_\nu(x-t) + J_{\nu-1}(x-s)J_{\nu+1}(x-t) \} f(t)\,dt$$
$$= 4\, f(s). \tag{2}$$

**2.** The object of this note is to show that the results (1) and (2) are true for another class of functions $f(x)$.

THEOREM 1. *If $f(x)$ be defined by*
$$f(x) = \int_a^b \frac{\sin(w-x)}{w-x} \phi(w)\, dw, \tag{3}$$
*where*
$$\int_a^b |\phi(\mu)|\, d\mu$$
*exists, then* (1) *and* (2) *are true.*

PROOF: Fox has proved the result
$$\int_s^{\infty} \left\{ (\nu-1)\frac{J_\nu(x-t)}{x-t} J_\nu(x-s) + \nu \frac{J_\nu(x-t)}{x-t} J_\nu(x-s) \right\} dx$$
$$= \frac{2}{\pi} \frac{\sin(s-t)}{s-t}. \tag{4}$$

Multiply both the sides of (4) by $f(t)$ and integrate from $-\infty$ to $\infty$.

Then,
$$\int_{-\infty}^{\infty} f(t)\, dt \int_s^{\infty} \left\{ (\nu-1)\frac{J_\nu(x-t)}{x-t} J_\nu(x-s) + \nu\frac{J_\nu(x-t)}{x-t} J_{\nu-1}(x-s) \right\} dx$$
$$= \frac{2}{\pi}\int_{-\infty}^{\infty} \frac{\sin(s-t)}{s-t} f(t)\, dt$$
$$= \frac{2}{\pi}\int_{-\infty}^{\infty} \frac{\sin(s-t)}{s-t}\, dt \int_a^b \frac{\sin(w-t)}{w-t} \phi(w)\, dw. \tag{5}$$
making use of (3).

Now, changing the order of integration in the repeated integral on the right side of (5), we get
$$\int_{-\infty}^{\infty} f(t)\,dt \int_s^{\infty} \left\{ (\nu-1)\frac{J_{\nu-1}(x-t)}{x-t} J_\nu(x-s) + \nu\frac{J_\nu(x-t)}{x-t} J_{\nu-1}(x-s) \right\} dx$$
$$= \frac{2}{\pi}\int_a^b \phi(w)\, dw \int_s^{\infty} \frac{\sin(s-t)}{s-t}\, \frac{\sin(w-t)}{w-t}\, dt, \tag{6}$$
the inversion being valid since both the integrals are absolutely convergent.

Now

$$\int_{-\infty}^{\infty} \frac{\sin(s-t)}{s-t} \frac{\sin(w-t)}{w-t} dt$$

$$=\frac{1}{s-w}\int_{-\infty}^{\infty} \frac{\sin(s-t)\sin(w-t)}{w-t} dt - \frac{1}{s-w}\int_{-\infty}^{\infty} \frac{\sin(s-t)\sin(w-t)}{s-t} dt.$$

Putting $w-t=y$ in the first and $s-t=z$ in the second, we have

$$\int_{-\infty}^{\infty} \frac{\sin(s-t)}{s-t} \frac{\sin(w-t)}{w-t} dt = \frac{1}{s-w}\int_{-\infty}^{\infty} \frac{\sin y}{y} \sin(y+s-w)\, dy$$

$$+\frac{1}{s-w}\int_{-\infty}^{\infty} \frac{\sin z}{z} \sin(z-s+w)\, dz$$

$$=\pi\frac{\sin(w-s)}{w-s}.$$

Hence (6) becomes, in virtue of (3)

$$\int_{-\infty}^{\infty} f(t)dt \int_{s}^{\infty}\left\{(\nu-1)\frac{J_\nu(x-t)}{x-t}J_\nu(x-s)+\nu\frac{J_\nu(x-t)}{x-t}J_{\nu-1}(x-s)\right\}dx$$

$$= 2f(s). \tag{7}$$

Hence by changing the order of integration on the left side of (7), we arrive at Fox's result.

2.1. Similarly we can prove (2) by starting with the result

$$\int_{s}^{\infty}\Big\{ J_{\lambda+1}(x-s)J_{\lambda-1}(x-t)+J_\lambda(x-s)J_\lambda(x-t)+J_\nu(x-s)J_\nu(x-t)$$

$$+J_{\nu-1}(x-s)J_{\nu+1}(x-t)\Big\}dx$$

$$=\frac{4}{\pi}\frac{\sin(s-t)}{s-t}.$$

2.2. THEOREM 2. *If $f(x)$ be defined by*

$$f(x)=\int_{a}^{b} \frac{\sin\mu(w-x)}{w-x}\phi(w)\, dw,$$

*where*

$$\int_{a}^{b} |\phi(w)|\, dw$$

*exists and $0<\mu\leqslant 1$, then (1) and (2) are true.*

To prove this, we make use of Hardy's* formula

$$\int_{-\infty}^{\infty} \frac{\sin m(t-x)}{t-x}\frac{\sin\mu(t-w)}{t-w} dt = \pi\frac{\sin\mu(w-x)}{w-x},\ 0<\mu\leqslant m,$$

put $m=1$, and proceed as before.

* *Loc. cit.*

# CANONICAL BASIS FOR IDEALS IN A POLYNOMIAL DOMAIN OVER A COMMUTATIVE RING WITH FINITE BASIS FOR IDEALS.

*By* R. VAIDYANATHASWAMY *and*
T. VENKATARAYUDU.

[Received 16 February 1938]

**1.** Let $A$ be a commutative ring with unit element and $A[x]$ denote the ring of polynomials in $x$ with coefficients from $A$. Hilbert's theorem is:—

*If every ideal in* A *has a finite basis, then every ideal in* $A[x]$ *also has a finite basis.*

The proof of this as given by Van der Waerden in his *Moderne Algebra* Bd. II gives us no information beyond the fact that every ideal in $A[x]$ has a finite basis. If we just reverse the argument in his proof we will be able to give actually a canonical basis for every ideal in $A[x]$ which will be found to be a powerful tool in several applications.

We assume the theorem that in a ring in which every ideal has a finite basis, a chain of ideals in which every ideal is a divisor of the previous one must be finite and conversely.

We prove now our principal

THEOREM A.—*Every ideal I in* $A[x]$ *has a basis in the form*

$$(a_{11}, a_{12}, \ldots, a_{1r_1}, a_{21}, a_{22}, \ldots, a_{2r_2}, \ldots, a_{t1}, a_{t2}, \ldots, a_{tr_t})$$

*where* $a_{k1}, a_{k2}, \ldots, a_{kr_k}$ *are polynomials in* $A[x]$ *whose highest coefficients form an ideal* $b_k$ *which is a true divisor of* $b_{k-1}$.

PROOF:—Let $n_1$ be the least degree of the polynomials in I, ($n_1$ may be zero). The highest coefficients of the polynomials of degree $n_1$ together with zero form an ideal in $A$, for if $\alpha$ and $\beta$ are the highest coefficients of the polynomials $a$, $b$ of degree $n$, $a-b$ is a polynomial of degree $n_1$, or is identically zero, and the highest co-

efficient of $a-b$ is $\alpha-\beta$ or 0. Further if $\alpha$ is the highest coefficient of $a$, $\lambda\alpha$ is the highest coefficient of the polynomial $\lambda a$. Hence the highest coefficients of the polynomials of degree $n_1$ together with zero form an ideal, say $b_1$, which by hypothesis has a basis, say $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r_1}$. Let $a_{11}, a_{12}, \ldots, a_{1r_1}$ be a set of polynomials in I whose highest coefficients are respectively $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r_1}$. We take $a_{11}, a_{12}, \ldots, a_{1r_1}$, as some basis elements in I. It follows from above that every polynomial in I of degree $n_1$ can be expressed in terms of $a_{11}, a_{12}, \ldots, a_{1r_1}$. For let

$$f = a_0 x^{n_1} + a_1 x^{n_1-1} + \ldots + a_{n_1}$$

be any polynomial in I of degree $n_1$. If $a_0=0$, $f$ itself is zero. Therefore $a_0 \neq 0$. $a_0$ is an element of the ideal $(\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r_1})$; let $a_0 = \lambda_1\alpha_{11} + \lambda_2\alpha_{12} + \ldots + \lambda_{r_1}\alpha_{1r_1}$.

The polynomial $\phi = \lambda_1 a_{11} + \lambda_2 a_{12} + \ldots + \lambda_{r_1} a_{1r_1}$ is of degree $n_1$ and the highest co-efficient is $a_0$. Hence $f-\phi$ is a polynomial of degree $< n_1$ and is hence identically zero.

Hence $f = \lambda_1 a_{11} + \lambda_2 a_{12} + \ldots + \lambda_{r_1} a_{1r_1}$, and therefore every polynomial in I of degree $n_1$ can be expressed in terms of $a_{11}, a_{12}, \ldots, a_{1r_1}$.

Now polynomials of degree $n$ $(n > n_1)$ occur in I. The highest coefficients of polynomials in I of degree $\leqslant n$ form an ideal $C$ in $A$. Since all elements of $b_1$ are elements in $C$, $C$ is a divisor of $b_1$. If all the elements of $C$ are elements in $b_1$, $C = b_1$. On the other hand if there is at least one element in $C$ which does not belong to $b_1$, we say that $C$ is a true divisor of $b_1$. Let $n_2$ be the least $n$ for which the ideal formed by the highest coefficients of polynomials of degree $\leqslant n_2$ form an ideal $b_2$ which is a true divisor of $b_1$. By hypothesis $b_2$ has a basis, say, $(\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2r_2})$. Let $a_{21}, a_{22}, \ldots, a_{2r_2}$ be a set of polynomials whose highest coefficients are $\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2r_2}$ respectively. We show in the first place that polynomials in I of degree $< n_2$ can be expressed in terms of $a_{11}, a_{12}, \ldots, a_{1r_1}$. Let $f = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ be a polynomial whose degree $n < n_2$. $a_0$ is therefore an element of $(\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1r_1})$. Let $a_0 = \lambda_1\alpha_{11} + \lambda_2\alpha_{12} + \ldots + \lambda_{r_1}\alpha_{1r_1}$. Take the polynomial $\phi_1 = \lambda_1 a_{11} + \ldots + \lambda_r \alpha_{1r_1}$. $f-\phi_1$ is a polynomial in I whose degree is $\leqslant n-1$ and continuing this process we find $f-\phi_1-\phi_2 \ldots - \phi_{n-n_1}$ is a polynomial in I of degree $n_1$ which, as we have already shown, can be expressed as a polynomial $\phi_{n-n_1-1}$ in terms of $a_{11}, \ldots, a_{1r_1}$. Hence $f = \phi_1 + \phi_2 + \ldots + \phi_{n-n_1} + \phi_{n-n_1-1}$.

We can show as in the previous case that any polynomial in I of degree $n_2$ can be expressed in terms of $a_{21}, a_{22}, \ldots a_{2r_2}$ and $a_{11}, a_{12}, \ldots, a_{1r_1}$, for if

$$f = a_0x^{n_2} + a_1x^{n_2-1} + \ldots + a_{n_2}$$

is a polynomial in I of degree $n_2$, $a_0$ is an element of the ideal $(\alpha_{21}, \alpha_{22}, \ldots, \alpha_{2r_2})$ and let

$$a_0 \equiv \mu_1\alpha_{21} + \mu_2\alpha_{22} + \ldots + \mu_{r_2}\alpha_{2r_2}.$$

Take the polynomial $\psi = \mu_1 a_{21} + \mu_2 a_{22} + \ldots + \mu_{r_2} a_{2r_2}$. It is of degree $n_2$ and the highest coefficient is $a_0$, and the polynomial $f - \psi$ is in I and of degree $< n_2$, and therefore can be expressed in terms of $a_{11}, a_{12}, \ldots a_{1r_1}$.

In continuing the construction as indicated above we get a chain of ideals $b_1, b_2, \ldots, b_{k-1}, b_k, \ldots$ in which each is a true divisor of the previous one and therefore the chain must be of finite length, say, let it stop with $b_t$. Let the basis of $b_t$ be $(\alpha_{t_1}, \alpha_{t_2}, \ldots, \alpha_{tr_t})$ and let $a_{t1}, a_{t2}, \ldots, a_{tr_t}$ be a set of polynomials in I whose highest coefficients are $\alpha_{t_1}, \alpha_{t2}, \ldots, \alpha_{tr_t}$ respectively. We prove as above that every element in I can be expressed in terms of $(a_{11}, a_{12}, \ldots, a_{1r_1}, a_{21}, a_{22}, \ldots, a_{2r_2}, \ldots, a_{t1}, a_{t2}, \ldots, a_{tr_t})$.

2. *Ideal theory of the integral polynomials.*

Since every ideal in $C$ is a principal ideal the canonical basis for ideals in $C\,[x]$ is simple. We have

THEOREM B. *Every ideal* I *in* $C[x]$ *can be put into the canonical form*

$$(Mx^{n_1}, M_1x^{n_1} f_1\,(x), M_2x^{n_1} f_1\,(x) f_2(x), \ldots),$$

*where* $M_r$ *is a factor of* $M_{r-1}$.

PROOF:—Let $n_1$ be the least degree of the polynomials in I. The highest coefficients of the polynomials in I of degree $n_1$ together with zero form an ideal say $(M)$. Let $a_1$ be a polynomial in I whose highest coefficient is $M$. Now $a_1 - Mx^{n_1} = 0$ and hence $a_1 = Mx^{n_1}$. Let $n_2$ be the least degree of the polynomials in I such that the highest coefficients of the polynomials in I of degree $\leqslant n_2$ form an ideal $(M_1)$ which is a true divisor of $M$. Let $\phi\,(x)$ be the polynomial of degree $n_2$ with highest coefficient $M_1$. If $M_1N_1 = M$, $N_1\phi(x) - Mx^{n_2}$ is a polynomial in I of degree $< n_2$ and hence $N_1\phi(x) - Mx^{n_2} = A_1Mx^{n_1}$ where $A_1$ is a polynomial in $C[x]$ and hence $\phi(x)$ is of the form $M_1x^{n_1}f_1(x)$. Similarly let $n_3$ be the least degree of the polynomials in I such that the highest coefficients of the polynomials of degree $\leqslant n_3$ form an ideal $(M_2)$

which is a true divisor of $M_1$, and let $\psi(x)$ be a polynomial in I whose highest coefficient is $M_2$. Let $M_2N_2=M_1$. Now the polynomial

$$N_2\psi(x)-M_1x^{n_1}f(x)\,x^{n_3-n_2}$$

is a polynomial of degree $<n_3$ and therefore

$$N_2\psi(x)-M_1x^{n_1}f_1(x)x^{n_3-\lambda_2}=A_1Mx^{n_1}+A_2M_1x_1^{n_1}f_1(x),$$

where $A_1$ and $A_2$ are two polynomials in $C[x]$. Hence
$N_2\,\psi(x)\equiv M_1\,x^{n_1}\,f_1\,(x).\,x^{n_3-n_2}+A_2\,M_1\,x^{n_1}\,f_1(x) \bmod (Mx^{n_1})$
and $\psi(x)$ is of the form $M_2x^{n_2}\,.\,f_1(x).f_2(x)\ (\bmod Mx^{n_1})$.

The process breaks after a finite number of steps and the theorem is established.

THEOREM 1. *Every prime ideal in* $C[x]$ *has one of the three forms:*

(1) $P=\Big(p, f\,(x)\Big)$, $p$ *a prime,* $f(x)$ *an irreducible polynomial.*

(2) $P=(p)$

*and* (3) $P=\Big(f\,(x)\Big)$.

THEOREM 2. *Every primary ideal in* $C[x]$ *has one of the three forms:*

$$(1)\ q=\Big(p^{\sigma_1}, p^{\sigma_2}.\,f_1^{\rho_1}(x), p^{\sigma_3}.\,f_1^{\rho_2}\,(x),\ldots, f_1^{\rho_t}(x)\Big),$$

*where* $p$ *is a prime and* $f(x)$ *is an irreducible polynomial*

$$\sigma_1>\sigma_2>\sigma_3\ldots, \rho_1<\rho_2<\ldots$$

(2) $q=(p^{\sigma})$

*and* (3) $q=\Big(f^{\rho}(x)\Big)$.

(1) requires proof, the other cases are evident. In the first instance $q$ is a primary ideal for $\Big(p, f(x)\Big)^{\lambda}\equiv_0(q)\equiv_0\Big(p,f(x)\Big)$ $\lambda>\sigma_1, \rho_t$ and $\Big(p, f(x)\Big)$ is a factorless ideal. Hence $q$ is primary.

On the other hand every primary ideal should be of this form. For, in constructing the canonical basis for it, it is obvious that the first term should be a power of a prime. If the second term is $p^{\sigma_2}.f_1^{\rho_1}(x).f_2^{\rho_2}(x)$ the subsequent basis elements must be multiples

of $f_1^{\rho_1}(x).f_2^{\rho_2}(x)$. Now $p^{\sigma_2}.f_1^{\rho_1}(x)\, f_2^{\rho_2}(x) \equiv o(q)$. But $p^{\sigma_2} f_2^{\rho_2}(x) \not\equiv o(\cdot q)$. Hence $f_1^{\rho_1}(x) \equiv o(q)$ for sufficiently great $\rho$ and hence

$$f_1^{\rho}(x) = p^{\sigma_1} + A_1 p^{\sigma_2} f_1^{\rho_1}(x).f_2^{\rho_2}(x) + \text{multiples of } f_1^{\rho_1}(x) f_2^{\rho_2}(x) \tag{1}$$

which is absurd, for whenever there is $f_1(x)$ there is also $f_2(x)$ with it. A relation of type (1) can therefore arise only when $A_1, A_2, \ldots$ are all zero and $f_1^{\rho}(x)$ is not a multiple of $p^{\sigma_1}$. Hence the second term should be $p^{\sigma_2}.f_1^{\rho_1}(x)$. For a similar reason, the third should be of the form $p^{\sigma_3}.f_1^{\rho_2}(x)$, and the last term should be a power of the irreducible polynomial $f_1(x)$, otherwise

$$f^{\rho}(x) = A_1 p^{\sigma_1} + A_2 p^{\sigma_2} f_1^{\rho_1}(x) + \ldots \tag{2}$$

and the right hand side is a multiple of $p$ and therefore for a relation of type (2) there must be a term which is independent of $p$.

# ON LAGUERRE POLYNOMIALS WHICH ARE SELF-RECIPROCAL IN THE HANKEL TRANSFORM

*By* R. S. VARMA, *Cawnpore*.

[Received 7 February 1938]

In a recent paper*, S. C. Mitra has shown that

$$\int_0^\infty z^{n-\frac{1}{2}}e^{-\frac{1}{4}z^2}D_{2n}(z)J_{n-1}(xz)\,dz$$

$$= (-)^n x^{n-\frac{1}{2}}e^{-\frac{1}{4}x^2}D_{2n}(x)$$

and

$$\int_0^\infty z^{n-\frac{1}{2}}e^{-\frac{1}{4}z^2}D_{2n-1}(z)J_n(xz)\,dz$$

$$= (-)^{n-1}x^{n-\frac{1}{2}}e^{-\frac{1}{4}x^2}D_{2n-1}(x).$$

More recently† I have shown that these results are particular cases of the general integral

$$\int_0^\infty y^{2l-n-1}e^{-\frac{1}{4}y^2}J_n(xy)W_{k,m}(\tfrac{1}{2}y^2)\,dy$$

$$= \frac{2^{l-n-1}x^n\,\Gamma(l+m+\frac{1}{2})\,\Gamma(l-m+\frac{1}{2})}{\Gamma(n+1)\,\Gamma(l-k+1)}\,{}_2F_2\left[\begin{matrix} l+m+\frac{1}{2},\ l-m+\frac{1}{2} \\ n+1,\ l-k+1 \end{matrix};-\tfrac{1}{2}x^2\right]$$

$$l\pm m+\tfrac{1}{2}>0. \qquad (1)$$

I now find that the relation (1) gives the following general

THEOREM. *The function*

$$\phi(x) = x^{2m+\mu+\frac{1}{2}}e^{-\frac{1}{2}x^2}L_\mu^m(\tfrac{1}{2}x^2)$$

$$\mu+2m+1>0$$

*is self-reciprocal or skew self-reciprocal in the Hankel transform of order* $\mu+2m$ *according as* $\mu$ *is even or odd.*

To prove this, we obviously see that when

$$l+m+\tfrac{1}{2} = n+1 \text{ or } l = n-m+\tfrac{1}{2}$$

* S. C. Mitra, 'On parabolic cylinder functions which are self-reciprocal in the Hankel transform', *Math. Zeit.*, 43 (1937), 205-11.

† R. S. Varma, 'Some infinite integrals involving Weber's parabolic cylinder functions', *Journ. Indian Math. Soc.* (2) 3 (1938), 25-33.

the generalised hypergeometric function on the right of (1) reduces to Kummer's function. Now since

$$L_n^m(x) = \frac{\Gamma(m+n+1)}{n!\,\Gamma(m+1)}\,{}_1F_1(-n\,;\,m+1\,;\,x)$$

$$= \frac{(-)^n}{n!}\,x^{-\frac{1}{2}(m+1)}e^{\frac{1}{2}x}W_{n+\frac{1}{2}m+\frac{1}{2},\,\frac{1}{2}m}(x)$$

we get from (1)

$$\int_0^\infty y^{n+1}e^{-\frac{1}{2}y^2}J_n(xy)L_\mu^{2m}(\tfrac{1}{2}y^2)\,dy$$

$$= (-)^\mu x^n e^{-\frac{1}{2}x^2}L_\mu^{n-\mu-2m}(\tfrac{1}{2}x^2). \qquad (2)$$

If we set $n=\mu+4m$ in (2), we obtain finally

$$\int_0^\infty \sqrt{xy}\,J_{\mu+2m}(xy)\,y^{2m+\mu+\frac{1}{2}}e^{-\frac{1}{2}y^2}L_\mu^m(\tfrac{1}{2}y^2)\,dy$$

$$= (-)^\mu x^{2m+\mu+\frac{1}{2}}e^{-\frac{1}{2}x^2}L_\mu^m(\tfrac{1}{2}x^2),$$

which is equivalent to the theorem stated above.

The following three special cases of the theorem are rather interesting:

Case (*i*) For $m=-\frac{1}{2}$ and $m=\frac{1}{2}$, we get Mitra's result given above.

Case (*ii*) For $m=0$, we obtain that the function

$$\phi(x) = x^{\mu+\frac{1}{2}}e^{-\frac{1}{2}x^2}L_\mu(\tfrac{1}{2}x^2)$$

is self-reciprocal or skew self-reciprocal in the Hankel transform of order $\mu$ according as $\mu$ is even or odd.

Case (*iii*) For $m=1$, we obtain that the function

$$\phi(x) = x^{\mu+\frac{1}{2}}e^{-\frac{1}{4}x^2}k_{2\mu+2}\left(\frac{x^2}{4}\right)$$

is self-reciprocal or skew self-reciprocal in the Hankel transform of order $\mu+2$ according as $\mu$ is even or odd.

# *ON THREE RATIONAL FUNCTIONS ON A RIEMANN SURFACE.

*By* K. S. SURYANARAYANAN, *Madras University.*

## I.

### 1. *Introductory.*

Let $y$ be an algebraic function of $z$ defined by the irreducible relation

$$F(y, z) \equiv A_0(z)y^n + A_1(z)y^{n-1} + \ldots + A_n(z) = 0 \qquad (1)$$

where the $A$'s are polynomials in $z$ of degree, say, $m$. The manifold of pairs of values $y, z$ which satisfy the given equation (1) constitute the *Riemann surface* of the algebraic function $y$, constructed in the usual manner. Any rational function of $y$ and $z$ is a rational function of position on this Riemann surface. The *order* of such a rational function is the number of places on the surface at which it takes an assigned value. In particular, $y$ and $z$ are rational functions of position on the surface of orders $m$ and $n$ respectively.

The totality of the rational functions on the Riemann surface defined by (1) forms a corpus. This corpus is the algebraic extension of the corpus $K(z)$ of rational functions of $z$ by the adjunction of the algebraic function $y$ of $z$ to $K(z)$. $y$ is called a *primitive* or *generating* element of the extended corpus inasmuchas every element of that corpus can be expressed as a rational function of $y$ and $z$. If, for example, $\eta$ be any other element of the corpus satisfying the irreducible relation $F(\eta, z) = 0$, where $F(\eta, z)$ is of degree $n$ in $\eta$, $\eta$ is also a primitive element of the corpus, or in other words, any element of the corpus is also a rational function of $\eta$ and $z$ so that there is a birational correspondence between $F(y, z) = 0$ and $F(\eta, z) = 0$.

Let us now suppose $x, y, z$ to be three rational functions of orders $l, m, n$ respectively on an assigned Riemann surface $R$. We can evidently give $z$† the role of the independent variable and

* I thank Dr. Vaidyanathaswamy for help in the preparation of this paper.

† Heinrich W. E. Jung, *Einführung in die Theorie der Algebraischen Funktionen einer Veranderlichen*, p. 66.

generate the corpus of rational functions on the Riemann surface as an algebraic extension of the corpus $K(z)$ of rational functions of $z$. (Geometrically this is equivalent to replacing the surface $R$ by a birationally and topologically equivalent surface with $n$ sheets, $n$ being the order of the rational function $z$). Suppose $x$ and $y$ are primitive elements of this corpus so that the irreducible relations

$$F_1(x, z)=0, \quad F_2(y, z)=0$$

connecting $x$, $y$ and $z$ are of degrees $n$ in $x$ and $l$ in $z$, $n$ in $y$ and $m$ in $z$ respectively. Let $\phi(x, y)$ be the $z$-resultant of $F_1$ and $F_2$, which is then of degrees $mn$ in $x$ and $ln$ in $y$. The present paper is concerned with the reducibility of $\phi(x, y)$.

In geometry, we know the case of Poncelet's theorem* wherein $\phi(x, y)$ splits into two factors, (two being the order of $z$), each of degree two in $x$ and $y$ where $x$ and $y$ themselves are of order two. The purpose of the present paper is to bring out the corpus-theoretic principle which is the explanation of the factorisability of $\phi$. The general result reached is as follows:

*Corresponding to every relative automorphism of the corpus of rational functions on the surface (i.e., automorphism which keeps the independent variable $z$ fixed), there is a factor $\psi(x, y)$ of $\phi(x, y)$ of degrees $l$, $m$ in $x$, $y$, which separates out from $\phi$.*

The Riemann surface with $z$ as the independent variable is $n$-sheeted. Each relative automorphism of the corpus of rational functions on this surface, therefore, is equivalent to a birational transformation of this surface into itself of such a sort that a point corresponds in this transformation to a certain one of the remaining $n-1$ points on the surface just above or below it. These special birational transformations of the surface into itself are called *deck-transformations.*

In II, I summarise the known theory of the relative automorphisms of any algebraic extension of a fundamental corpus and apply the result to the corpus of rational functions on a Riemann surface, considered as an algebraic extension of $K(z)$. In III, I prove the main result of the paper and in IV, I consider some applications.

* R. Vaidyanathaswamy, A Postscript to Poncelet's Theorem. *Proc. L. M. S.* (2), 27.

## II

**2.** *Relative automorphisms of an algebraic extension of a fundamental corpus.*

Let $\Delta_1$ and $\Delta_2$ be any two algebraic extensions of a fundamental corpus $\Delta$. $\Delta_1$ and $\Delta_2$ are said to be 'isomorphic relatively to $\Delta$' or briefly in *relative isomorphism*, when there is a (1, 1) correspondence between the elements of $\Delta_1$ and $\Delta_2$, preserving addition and multiplication, which leaves the elements of $\Delta$ unaltered. If further $\Delta_1$ is identical with $\Delta_2$, the relative isomorphism becomes a relative automorphism.

Let $\Delta_1$ and $\Delta_2$ be algebraic extensions of a fundamental corpus $\Delta$, with a relative isomorphism $\Sigma$. In this paper, we assume that all algebraic extensions admit primitive elements.* Then $\Delta_1$ is an algebraic extension of $\Delta$ by the adjunction of $\alpha$ to it, so that $\Delta_1 = \Delta(\alpha)$, where $\alpha$ satisfies an irreducible equation $f(\alpha)=0$, $f(\alpha)$ having its coefficients in $\Delta$. $\alpha$, then, is a primitive element of $\Delta_1$, and if $\beta$ in $\Delta_2$ corresponds to $\alpha$ in the relative isomorphism $\Sigma$, $\beta$ should also be a primitive element of $\Delta_2$, and $\beta$ too satisfies the algebraic relation $f(\beta)=0$ as the co-efficients of $f(\beta)$ are unaltered in the isomorphism. Thus $\Delta_1$ and $\Delta_2$ arise by adjunction of conjugate algebraic elements to the fundamental corpus and therefore are themselves conjugate algebraic extensions of the fundamental corpus. It is also evident that $\Sigma$ carries every element of $\Delta_1$ into its conjugate element in $\Delta_2$. Conversely, if all the conjugate algebraic extensions of the fundamental corpus corresponding to the roots of $f(x)=0$ are distinct, there can be only one relative isomorphism between $\Delta_1$ and $\Delta_2$, namely, that in which $\alpha$ corresponds to $\beta$, since, by hypothesis, $\beta$ is the only primitive element in $\Delta_2$ conjugate to $\alpha$.

The polynomial $f(x)$ of degree $n$, defines $n$ algebraic extensions of the fundamental corpus $\Delta$ and is irreducible in $\Delta$. It has, therefore, $n$ distinct roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. But even though the roots are distinct, it may well happen that the algebraic extensions are not all distinct. For this case we have

THEOREM 1. *If exactly $r$ of the conjugate corpuses coalesce with $\Delta(\alpha_1)$, then the $n$ corpuses $\Delta(\alpha_i)$ coalesce in groups of $r$ so that $n/r$ of them are distinct and $r$ is a divisor of $n$.*

*Further, each of the $n/r$ distinct corpuses $\Delta(\alpha_i)$ has a group of $r$ relative automorphisms, and these $n/r$ groups are (1, 1) isomorphic with one another.*

* For the condition that the algebraic extension of a corpus may admit primitive elements, see Van der Waerden, *Moderne Algebra*, Band I, p. 120.

PROOF: Suppose $\Delta(\alpha_1) = \Delta(\alpha_2) = \ldots = \Delta(\alpha_r) \neq \Delta(\alpha_i)$ $(i = r+1, \ldots, n)$. By what has been proved, there is a relative isomorphism betwen $\Delta(\alpha_1)$ and $\Delta(\alpha_{r+1})$, in which $\alpha_1$ corresponds to $\alpha_{r+1}$. Since $\alpha_2, \ldots, \alpha_r$ are primitive elements of $\Delta(\alpha_1)$ satisfying the equation $f(x)=0$, they must correspond in this isomorphism to primitive elements of $\Delta(\alpha_{r+1})$ also satisfying the equation $f(x) = 0$, that is, to elements which are conjugate to $\alpha_2, \ldots, \alpha_r$. Let the elements to which they correspond be $\alpha_{r+2}, \ldots, \alpha_{2r}$. Then $\Delta(\alpha_{r+1}) = \Delta(\alpha_{r+2}) = \ldots = \Delta(\alpha_{2r})$. By reversing the above argument we can show that $\Delta(\alpha_{r+1})$ does not coalesce with any other conjugate corpus. By continuing this argument we show finally that the $n$ conjugate corpuses $\Delta(\alpha_i)$ coalesce in groups of $r$ so that $n/r$ of them are distinct and that $r$ is a divisor of $n$.

Since $\alpha_1, \alpha_2, \ldots, \alpha_r$ are mutually distinct, $\Delta(\alpha_1)$ has $r$ relative automorphisms which respectively carry $\alpha_1$ into $\alpha_1, \alpha_2, \ldots, \alpha_r$. Since further $\Delta(\alpha_1) \neq \Delta(\alpha_i)$ $(i=r+1, \ldots)$ by hypothesis, it has no other relative automorphisms. These $r$ relative automorphisms must evidently form a group which can be represented as a permutation group of the $r$ symbols $(\alpha_1, \alpha_2, \ldots, \alpha_r)$. Since $\Delta(\alpha_1)$ and $\Delta(\alpha_{r+1})$ are relatively isomorphic, the groups of their relative automorphisms are abstractly identical. We can thus speak of the group of relative automorphisms associated with an irreducible relation $f(x) = 0$, meaning thereby the group of automorphisms of any one of the algebraic extensions of the fundamental corpus by the adjunction of a root of $f(x) = 0$.

3. *Application to the case of the algebraic function of a complex variable.*

We shall now apply the above theory to the case of the algebraic function of a complex variable $z$. We shall take for the fundamental corpus $\Delta$, the corpus $\Delta(z)$ of all complex rational functions of the complex variable $z$. The irreducible relation in $\Delta(z)$ corresponding to $f(x) = 0$ is of the form

$$F(x, z) \equiv A_0(z)x^n + A_1(z)x^{n-1} + \ldots + A_n(z) = 0$$

where the $A$'s are polynomials in $z$ of degree, say, $m$. The manifold of pairs of values $z, x$ satisfying this equation constitute the Riemann surface constructed in the usual manner; and the surface is $n$-sheeted if we take $z$ to be the independent variable. A rational function of position on this surface is a rational function in the ordinary sense of $x$ and $z$. All such rational functions of position on the surface, therefore, form a corpus.

But in order to extend as before the fundamental corpus $\Delta(z)$ by the adjunction of a root of $F(x, z) = 0$, we want the $n$ roots

of this equation, say, $x_1, x_2, \ldots, x_n$ as $n$ distinct entities. But the distinctness of each of these roots has become obliterated in the concept of the Riemann surface. The same rational function $x$ on the Riemann surface takes these values at the $n$ points having the same $z$-coordinate. But if we cut up all the passages which connect the various sheets so that no point can move from one sheet to another, each sheet contains only one point with a given $z$-coordinate, in fact the sheets are really $z$-planes with cuts along the lines joining the branch points of $x$ *qua* function of $z$. Therefore the rational function $x$, being a rational function of position, takes only one value for a given $z$ on a sheet, and the value $x_i$ is taken only on the $i$-th sheet. Thus, the roots have been exhibited as single-valued functions of $z$ on the cut sheets, which cannot pass over into one another. These roots, therefore, may be adjoined to $\Delta(z)$ to get the $n$ algebraic extensions which may or may not all be distinct. By our general result, these $n$ extensions are in relative isomorphism with one another by means of the correspondence $x_i \rightarrow x_j, z \rightarrow z$. We now prove the following result:

*Each of the $n$ corpuses $\Delta(z, x_i)$ is also in relative isomorphism with the corpus of rational functions on the Riemann surface.*

For, the one-valued function of position $x$ takes the same values at points of the $i$-th sheet of the Riemann surface as the one-valued function $x_i$ at those points of the separated $i$-th sheet. If we patch up the cuts and extend analytically the value of the function $x_i$ along all possible paths throughout the Riemann surface, $x_i$ takes the same value at points of the Riemann surface as the rational function $x$ does. The one-valued function of position $z$ on the separated $i$-th sheet takes the same values at points of the restored Riemann surface as the rational function $z$ on the surface. Also any rational function $R(z, x_i)$ of $z$ and $x_i$, treated in the same way, takes the same values on the uncut surface as the rational function $R(z, x)$. Hence the relative isomorphism between $\Delta(z, x_i)$ and the corpus of rational functions on the Riemann surface follows.

As a consequence of this relative isomorphism, it follows that if the corpuses $\Delta(z, x_i)$ coalesce in groups of $r$ ($r$, a divisor of $n$) in accordance with Theorem 1, so that $\Delta(z, x_i)$ admits a group $G_r$, of order $r$, of relative automorphisms, then the corpus of rational functions on the Riemann surface also admits the group $G_r$ of relative automorphisms. Since a position on the Riemann surface may be identified with a pair of values of $x, z$ which satisfy the equation $F(x, z) = 0$, a relative automorphism of the corpus of

rational functions on the surface may be defined by $x' \to x$, $z \to z$; $F(x, z) = F(x', z) = 0$. A relative automorphism of the corpus of rational functions on the surface must, therefore, be interpreted as a deck-transformation $a \to g(a)$ of positions on the surface such that the rational function $x'$ corresponding to $x$, takes the same value at $g(a)$ as the function $x$ takes at $a$. Thus the Riemann surface admits the group $G_r$ of deck-transformations. In particular if $r = n$, the equation $F(x, z) = 0$ is Galoisian over $\Delta(z)$ and the associated Riemann surface is *regular*,* admitting a group of $n$ deck-transformations so that corresponding to any two points having the same $z$-coordinate, we have a deck-transformation of the surface carrying one of them into the other.

## III

4. *Factorisability of the resultant connected with three rational functions $x, y, z$.*

If $x$ and $y$ are rational functions of orders $m$ and $l$ on the Riemann surface defined by $F(x, z) = 0$, then to each value of $x$ there are $m$ positions on the surface and therefore $m$ values of $y$, while to each value of $y$ there are $l$ values of $x$. Hence there is an algebraic relation $\psi(x, y) = 0$ connecting $x, y$ of degree $l$ in $x$ and $m$ in $y$. The polynomial $\psi$ may or may not be irreducible.

Hence also there is a relation $F'(y, z) = 0$ connecting $y$ and $z$, of degree $n$ in $y$ and $l$ in $z$. We assume this relation to be irreducible, so that $y$ is also a primitive element of the corpus of rational functions on the surface and the relations $F(x, z) = 0$, $F'(y, z) = 0$ can be birationally transformed into each other. Denote the $z$-resultant of $F(x, z)$, $F'(y, z)$ by $\phi(x, y)$ so that $\phi$ is of degree $nl$ in $x$ and $nm$ in $y$.

We now prove

THEOREM 2. *$\psi(x, y)$ is a factor of the eliminant $\phi(x, y)$.*

PROOF: The relation $\psi(x, y) = 0$ connects the values of $x, y$ at the same position on the Riemann surface, while the relation $\phi(x, y) = 0$ (from the meaning of elimination) connects the respective values of $x, y$ at two positions with the same $z$, i.e. directly above or below each other. Hence $\psi(x, y) = 0$ implies $\phi(x, y) = 0$. Hence $\psi(x, y)$ is a factor of $\phi(x, y)$.

This theorem may be generalised as

THEOREM 3. *To each deck-transformation of the Riemann surface associated with the birationally equivalent irreducible equations $F(x, z) = 0$, $F'(y, z) = 0$, there corresponds a factor*

* Kerekjarto, *Vorlesungen uber Topologie* I, p. 162.

JL
BmQ1N34
N34.3.2
129108
600 008

*$\psi_1(x, y)$ of degree $l$ in $x$ and $m$ in $y$ of the $z$ resultant $\phi(x, y)$ of $F, F'$.*

The previous theorem is the particular case of this, corresponding to the identical deck-transformation.

PROOF: Suppose we have a deck-transformation $a \to g(a)$. We have seen that to each such deck-transformation there is a relative automorphism $y \to y_g$ of rational functions on the surface such that $y_g$ takes the same value at $g(a)$ as $y$ takes at $a$. In other words, to each point $a$, there is a point $g(a)$ with the same $z$ such that the value of $y$ at $a$ is the same as the value of $y_g$ at $g(a)$. So the orders of the rational functions $y$ and $y_g$ are the same. The two rational functions $x$ and $y_g$ are connected by the relation $\psi_1(x, y_g) = 0$, (of degree $l$ in $x$ and $m$ in $y$) the values of $x$ and $y_g$ being taken in the same position, say, $g(a)$. Since $y_g$ takes the same value at $g(a)$ as $y$ at $a$, $\psi_1(x, y) = 0$ connects the values of the rational functions $y, x$ at $a, g(a)$ respectively. As before, since $a$ and $g(a)$ have the same $z$-coordinate, $\psi_1(x, y) = 0$ connects the values of $x$ and $y$ at points having the same $z$-coordinate, and hence $\psi_1(x, y) = 0$ implies $\phi(x, y) = 0$, so that $\psi_1$ is a factor of $\phi$.

5. *Irreducibility of the factors $\psi$.*

Each relation $\psi_1(x, y_g) = 0$ connects the respective values of the rational functions $x, y_g$ at $g(a)$ on the Riemann surface where $a \to g(a)$ defines a deck-transformation. Therefore by a known* result in the theory of algebraic functions, $\psi_1(x, y_g)$ is either an irreducible polynomial or a power of an irreducible polynomial. Therefore, $\psi_1(x, y)$ which when equated to zero connects the values of $y, x$ at $a, g(a)$ respectively, is either an irreducible polynomial or a power of an irreducible polynomial. The condition that $\psi_1(x, y)$ is irreducible is contained in

THEOREM 4. *If $P(x, z_1), Q(x, z_2)$ be any two points on the Riemann surface having the same $x$-coordinate, the condition for $\psi_1(x, y)$ (which when equated to zero connects the values of $x$, $y$ at $a, g^{-1}(a)$, $g^{-1}$ being the inverse of the deck-transformation $g$) to be irreducible, is that $y$ does not take the same value at $g^{-1}(P)$ and $g^{-1}(Q)$.*

PROOF: $y$ takes the same value at $g^{-1}(a)$ as $y_g$ at $a$. Let $x$ take the value $x$ at the points $P(x, z_1), Q(x, z_2), \ldots, W(x, z_m)$.

* Appell and Goursat, *Fonctions Algebriques*, p. 257.

If $y_g$ takes the same value at more than one of these points, say at $r$ of them, then the relation $\psi_1(x, y_g) = 0$ is reducible* and $\psi_1(x, y_g)$ is a perfect $r$-th power of an irreducible polynomial so that $\psi_1(x, y)$ will be a perfect $r$-th power of an irreducible polynomial. So for irreducibility of $\psi_1$, $y_g$ must not take the same value at any two points of the sort $P, Q, \ldots, W$ at which $x$ takes the same value, that is, for irreducibility of $\psi_1$, $y$ must not take the same value at any two of the points $g^{-1}(P), g^{-1}(Q) \ldots, g^{-1}(W)$.

In the case in which the factor $\psi_1$, corresponding to the deck-transformation $a \rightarrow g(a)$ is *irreducible*, we bring out the essentially identical nature of the branch points of $y$ and $z$ considered as functions of $x$, by means of

THEOREM 5. *The algebraic functions of $x$ defined by $\psi_1(x,y) = 0$ and $F(x, z) = 0$ have identical branch points of the same orders each.*

PROOF: Let $S$ be the Riemann surface of $F(x, z) = 0$ with $x$ as the independent variable, and let $S'$ be the Riemann surface of $\psi_1(x, y) = 0$ also with $x$ as the independent variable. Since $\psi_1(x, y)$, by hypothesis, is irreducible, there is a $(1, 1)$ birational correspondence between the points of $S$ and $S'$. Let $a$ be a branch point of $z$ *qua* function of $x$ of order $r-1$. Then $z$ can be expanded in the form

$$z = (x-a)^{s/r}[\alpha_0 + \alpha_1(x-a)^{1/r} + \ldots].$$

Since $y = R(x, z)$, a rational function of $z$ and $x$, $y$ is also capable of being expanded in powers of $(x-a)^{1/r}$. It might be argued that in the substitution for $z$ in $R(x, z)$, all powers of $(x-a)^{1/r}$ may get suppressed except those of $(x-a)^{p/r}$ where $r = p\delta$ ($p$, $\delta$ are integers) so that $y$ is expressible in powers of $(x-a)^{1/\delta}$ itself. This is untenable, because then $z$ which is a rational function of $x$ and $y$ will be capable of expansion in powers of $(x-a)^{1/\delta}$, or of $(x-a)^{1/\varepsilon}$ where $\delta = \gamma\varepsilon$ ($\gamma$ and $\varepsilon$ are integers) for the same reason as was considered hypothetically in the previous sentence; which in either case contradicts the hypothesis. So $y$ is also expressible in powers of $(x-a)^{1/r}$ only, and $a$ is a branch point of $y$ *qua* function of $x$ of order $r-1$.

If $\psi_1$ and $\psi_2$ be two irreducible factors of the $z$-resultant, the functions $y$ of $x$ defined by $\psi_1 = 0$, $\psi_2 = 0$ have also only identical

* Appell and Goursat, *loc. cit.*, p. 258.

branch points of the same orders since each of these functions has branch points identical with those of $z$ and of the same orders.

Results similar to the above are also obtained for the functions $z$ and $x$ considered as algebraic functions of $y$ given by $F'(y, z) = 0$; $\psi_1(x, y) = 0$.

6. *The distinctness of the factors $\psi$.*

Let the relation $\psi_1 = 0$ connect the values of $y$, $x$ at $a$, $g(a)$ respectively and let $\psi_1 \equiv [\psi']^k$ so that $\psi'$ is a polynomial of degree $l/k$ in $x$ and $m/k$ in $y$, and $k$ is a divisor of $l$ and $m$. If $k = 1$, this becomes the case where $\psi_1$ is irreducible. If the value of the rational function $y$ be denoted by $y(a)$ at $a$ and that of the rational function $x$ at $g(a)$ by $x(g)$, corresponding to the value $y(a)$ of $y$ in $\psi_1 = 0$ the values of $x$ will be $x(g) = x_1, x_2, \ldots, x_{l/k}$.

We first prove the following result.*

*No two of the roots $x(g) = x_1, x_2, \ldots, x_{l/k}$ are the values assumed by the rational function $x$ at points $a$, $g(a)$, where $a \to g(a)$ defines a deck-transformation.*

For, the rational function $y$ takes the value $y(a)$ at, say, $a_1, a_2, \ldots, a_l$. No two of these points, say, $a$, $a_i$ define a deck-transformation $a \to a_i (= g(a))$ since in that case $y$ and $z$ will take the same values at two distinct points of a Riemann surface which is birationally equivalent to that of $F'(y, z) = 0$. Since $\psi_1 = 0$ connects the values of the rational functions $y$, $x$ at $a$, $g(a)$ respectively, $x\{g(a_2)\}$, the value of the rational function $x$ at $g(a_2)$, should be among $x_2, \ldots, x_{l/k}$. Let $x\{g(a_2)\} = x_2$. In the same way we assume that $x\{g(a_3)\} = x_3, \ldots, x\{g(a_{l/k})\} = x_{l/k}$. $x\{g(a_{l/k+1})\}$ is again one of the values $x_1, x_2, \ldots, x_{l/k}$ and so on. So since no two of the $a$'s define a deck-transformation, $x_1, x_2, \ldots, x_{l/k}$ do not contain values assumed by $x$ at points of the sort $a_k$, $g(a_k)$, where $g$ is a deck-transformation; which is the result to be proved.

We are now in a position to prove

THEOREM 6. *If $\psi_1(x, y)$, $\psi_2(x, y)$ be factors of the $z$-resultant corresponding to the deck-transformations $a \to g_1(a)$, $a \to g_2(a)$ respectively, $\psi_1$ and $\psi_2$ cannot have a non-constant common factor.*

* In this result and in the following theorem, the proof is practically the same for the case where $\psi_1$ is irreducible, if we put $k = 1$.

PROOF: Suppose $\psi_1$ is a power of an irreducible polynomial so that $\psi_1 = [\psi']^k$. If $\psi_2$ is to have a non-constant common factor with $\psi_1$, the factor must be $\psi'$ or some power of $\psi'$, so that $\psi_2 = [\alpha\psi']^k$ where $\alpha$ is a constant, as otherwise $\psi_2$ will have distinct polynomial factors. Let the value of $y$ at $a$ be $y(a)$. Corresponding to the value $y(a)$ of $y$ in $\psi_1 = 0$, the values of $x$ are, say, $x_1, x_2, \ldots, x_{l/k}$. Since $\psi_2 = \alpha^k \psi_1$, the values of $x$ corresponding to the value $y(a)$ of $y$ in $\psi_2 = 0$ are also $x_1, x_2, \ldots, x_{l/k}$. From the definition of $\psi_1$, one of these values is $x\{g_1(a)\}$ and from that of $\psi_2$, one of these is again $x\{g_2(a)\}$. It follows that either at least two of the roots of the equation $\psi_1\{x, y(a)\} = 0$ are the values of the rational function $x$ at $g_1(a)$, $g_2(a)$ i.e. at $g_1(a)$, $g_2 g_1^{-1}\{g_1(a)\}$, or $x\{g_1(a)\} = x\{g_2 g_1^{-1}(g_1(a))\}$. The former contradicts the result proved in the previous paragraph and the latter is untenable since then there will be two distinct points $(x, z)$ on the Riemann surface.

7. *The Extreme Cases.*

In the case in which $F(x, z) = 0$ is Galoisian over $\Delta(z)$, the Riemann surface of $F(x, z) = 0$ with $z$ as the independent variable is regular and admits the maximum group of $n$ deck-transformations. The $z$-resultant of $F$, $F'$ therefore, factorizes into the maximum number of $n$ factors of the type mentioned in Theorem 3. *This case we call the case of maximum reducibility of* $\phi(x, y)$.

On the other hand, if $F(x, z) = 0$ has only one deck-transformation, namely, the identical one which it always has, there is only one factor of the type $\psi$. *Since there is always the identical deck-transformation,* $\phi(x, y)$ *has always a factor of the type* $\psi$.

IV

8. *Applications—Poncelet's Theorem* and its Extension.*

Here we shall examine two particular examples illustrating our main theorem of reducibility of $\phi(x, y)$.

($a$) One is the geometrical problem of Poncelet's Theorem*.

Let $x$, $y$, $z$ be three variable points on a conic $E$, such that the straight lines $xz$, $yz$ touch two conics $F_1$, $F_2$ respectively.

* R. Vaidyanathaswamy, *loc. cit.*

The envelope of $xy$ is in general a curve $\phi$ of class eight. Poncelet's theorem asserts that if $F_1$ and $F_2$ have the same four points $p_1, p_2, p_3, p_4$ in common with $E$, the envelope $\phi$ splits into two conics $\phi_1, \phi_2$ each counted twice and passing through the same four points $p_1, p_2, p_3, p_4$.

If now we also let $x, y, z$ represent three points on $E$ parametrically, then $(x, z)$ and $(y, z)$ are connected by two irreducible symmetric doubly quadratic relations $F_1(x, z)=0$ and $F_2(y, z)=0$. Further $F_1$ and $F_2$ are so related that they have the same discriminant points $p_1, p_2, p_3, p_4$. The algebraic statement of Poncelet's theorem, therefore, reduces to that the $z$-resultant of two irreducible symmetric double quadratics $F_1(x, z)$, $F_2(y, z)$ with identical discriminant-points splits into two other symmetric double quadratics $\phi_1(x, y)$, $\phi_2(x, y)$ with the same discriminant points as $F_1, F_2$.

This statement can be proved by applying our reducibility theorem as follows:

Let $$F_1 \equiv Ax^2-2Bx+C = 0$$

where $A, B, C$ are quadratics in $z$, so that

$$x = (B \pm \sqrt{\Delta})/A,$$

$\Delta$ being the $x$-discriminant of $F_1$; or $x = P_0 \pm P_1\sqrt{\Delta}$, $P_0, P_1$ being rational functions in $z$. So $\sqrt{\Delta}$ is a rational function of $x$ and $z$.

Similarly $$y = P'_0 \pm P'_1\sqrt{\Delta'},$$

$\Delta'$ being the $y$-discriminant of $F_2$, and $P'_0$, $P'_1$ rational functions of $z$ obtained from $F_2$ in the same way as $P_0, P_1$ are obtained from $F_1$. Therefore, $y$ is a rational function of $z$ and $\sqrt{\Delta'}$. If $\Delta \equiv k\Delta'$ where $k$ is a constant, which is the case when the discriminant points of $F_1$ and $F_2$ are identical, then $y$ is a rational function of $z$ and $x$. In the same way $x$ is a rational function of $z$ and $y$ so that a birational correspondence is obtained between $F_1$ and $F_2$, and $x, y, z$ are rational functions on the Riemann surface of $F_1 = 0$ with $z$ as the independent variable. $x$ and $y$ are then primitive elements of the corpus of rational functions on the surface.

The roots of $F_1 = 0$ for a value $z$ of $z$ are $P_0 \pm P_1\sqrt{\Delta}$ and both of these are found in the corpus $K(z, \sqrt{\Delta})$ which is the algebraic extension of the corpus $K(z)$ of rational

functions of $z$ by the adjunction of $\sqrt{\Delta}$. So this is Galoisian over $K(z)$ and hence has the maximum number of two automorphisms. It follows therefore that the corpus of rational functions on the Riemann surface, being isomorphic with $K(z, \sqrt{\Delta})$, also has two automorphisms which we are to identify with a group of two deck-transformations of the surface. The $z$-resultant of $F_1$ and $F_2$ therefore contains two symmetric double quadratics as factors.

(*b*) The other example is the extension of the previous one to the hyperelliptic case.

Let $F_1(x, z)$, $F_2(y, z)$ be irreducible polynomials of the second degree in $x$ and $y$ respectively. Let $z$ be of degree $m$ in $F_1$ and $p$ in $F_2$.

The procedure of the first example holds here also.

If the discriminant points are identical, the $x$ and $y$ discriminants of $F_1$ and $F_2$ respectively are identical but for a constant factor. $y$ is therefore a rational function of $x$ and $z$, also $x$ is a rational function of $y$ and $z$, i.e. there is a birational correspondence between $F_1$ and $F_2$. Therefore $x, y, z$ are rational functions on the Riemann surface of $F_1 = 0$, of which we can make $z$ the independent variable. $x$ and $y$ are as before primitive elements of the corpus of rational functions on the surface.

If again $\Delta$ be the $x$-discriminant of $F_1$, $K(z, \sqrt{\Delta})$, the algebraic extension of $K(z)$ the corpus of rational functions of $z$ by the adjunction of $\sqrt{\Delta}$ contains both roots of $F_1 = 0$ and therefore has two automorphisms. The corpus of rational functions on the surface, therefore, has a group of two automorphisms so that the surface has a group of two deck-transformations. So the $z$-resultant has two factors $\psi_1, \psi_2$, each of degree $p$ in $x$ and $m$ in $y$.

# INFINITESIMAL DEFORMATION OF RULED SURFACES

*By* RAM BEHARI, *University of Delhi.*

[Received 27 January 1938]

The problem of infinitesimal deformation of a ruled surface or the equivalent problem of determining a surface which corresponds to a given ruled surface with orthogonality of corresponding elements has been investigated by Goursat,* Darboux† and Haag.‡

The object of this paper is first to deal with the general problem of infinitesimal deformation of any surface and then to apply the results to the case of a ruled surface.

Let $x$, $y$, $z$ be the coordinates of a surface $S$, then the coordinates of a surface $S'$ which is an infinitesimal deformation of $S$ are given by

$$x' = x+\varepsilon\xi, \quad y' = y+\varepsilon\eta, \quad z' = z+\varepsilon\zeta,$$

where $\varepsilon$ is a small quantity whose second and higher powers are negligible, and $\xi$, $\eta$, $\zeta$ are functions of the current superficial variables $u$ and $v$.

The necessary and sufficient condition for the applicability of the two surfaces $S$ and $S'$, viz.

$$dx'^2+dy'^2+dz'^2 = dx^2+dy^2+dz^2,$$

gives

$$dx\, d\xi+dy\, d\eta+dz\, d\zeta = 0.$$

Since $\xi$, $\eta$, $\zeta$ are functions of $u$ and $v$, they can be regarded as the coordinates of a point on an unknown surface and then $d\xi$, $d\eta$, $d\zeta$ give an arc-element on the surface. Therefore, this equation shows that the problem of infinitesimal deformation of surfaces is the same as that of finding a surface which corresponds to a given surface with orthogonality of linear elements.

* 'Sur les equations lineaires et la methode de Laplace'. *American Journal of Mathematics*, Vol. 18; also, 'Sur les lignes asymptotiques', *Comptes Rendus* (1896), 593.

† *Lecons sur la Theorie Generale des Surfaces*, Vol. IV, p. 25.

‡ 'Sur la deformation infiniment petite des surfaces reglees' *Nouvelles Annales de Mathematique*, (1912), 312-331, 337-358.

Referred to asymptotic lines $u=$ const. and $v=$ const. as the parametric curves, the equations of the surface $S$ are given by

$$\left.\begin{aligned} x &= \int\left(\theta_2\frac{\partial\theta_3}{\partial u}-\theta_3\frac{\partial\theta_2}{\partial u}\right)du-\left(\theta_2\frac{\partial\theta_3}{\partial v}-\theta_3\frac{\partial\theta_2}{\partial v}\right)dv,\\ y &= \int\left(\theta_3\frac{\partial\theta_1}{\partial u}-\theta_1\frac{\partial\theta_3}{\partial u}\right)du-\left(\theta_3\frac{\partial\theta_1}{\partial v}-\theta_1\frac{\partial\theta_3}{\partial v}\right)dv,\\ z &= \int\left(\theta_1\frac{\partial\theta_2}{\partial u}-\theta_2\frac{\partial\theta_1}{\partial u}\right)du-\left(\theta_1\frac{\partial\theta_2}{\partial v}-\theta_2\frac{\partial\theta_1}{\partial v}\right)dv, \end{aligned}\right\} \qquad (\mathrm{I})$$

where $\theta_1$, $\theta_2$, $\theta_3$ are three particular solutions of

$$\frac{\partial^2\theta}{\partial u\partial v}=\lambda\theta, \qquad (\mathrm{II})$$

satisfying also the relation

$$\theta_1^2+\theta_2^2+\theta_3^2=\sqrt{-RR'}$$

where $R$ and $R'$ denote the principal radii of curvature of the surface $S$ at $(u, v)$, $\lambda$ being any function of $u$ and $v$.*

Now the surface $S'$ which is an infinitesimal deformation of the surface $S$ can be determined by finding $\xi$, $\eta$, $\zeta$ which are given by the relation

$$dx.d\xi+dy.d\eta+dz.d\zeta=0. \qquad (1)$$

This equation is equivalent to

$$\Sigma x_1\xi_1=0,\ \Sigma x_2\xi_2=0,\ \Sigma x_1\xi_2+\Sigma x_2\xi_1=0. \qquad (2)$$

Introducing a function $\phi$ defined by the relation

$$2V\phi=\Sigma x_1\xi_2-\Sigma x_2\xi_1,$$

we have

$$\Sigma x_1\xi_1=0,\quad \Sigma x_1\xi_2=V\phi,\quad \Sigma x_2\xi_1=-V\phi,\quad \Sigma x_2\xi_2=0 \qquad (3)$$

We know that $\phi$ is determined by the partial differential equation of the second order

$$\frac{\partial}{\partial u}\left(-\frac{M}{KV}\phi_2\right)+\frac{\partial}{\partial v}\left(-\frac{M}{KV}\phi_1\right)-\frac{2FM}{V}\phi=0, \qquad (4)$$

since $L=N=0$, and that

$$\xi_1=\frac{M}{KV}(X\phi_1-X_1\phi) \qquad (5)$$

and

$$\xi_2=-\frac{M}{KV}(X\phi_2-X_2\phi) \qquad (6)$$

with similar expressions for $\eta_1$, $\zeta_1$ and $\eta_2$, $\zeta_2$.† $\xi$, $\eta$, $\zeta$ are then given by

$$\int\xi_1du+\xi_2dv,\ \int\eta_1du+\eta_2dv\ \text{ and } \int\zeta_1du+\zeta_2dv.$$

* See Darboux, *Theorie des Surfaces*, Vol. IV, p. 24.

† Forsyth, *Diff. Geom.* pp. 402-403.

The differential equation (4) which gives $\phi$ can be written in a more convenient form from which three particular integrals are immediately obtained, as follows:—

Let $K=-\frac{M^2}{V^2}=-\frac{1}{\rho^2}$ where $\rho$ is the radius of total curvature, then (4) becomes

$$\frac{\partial}{\partial u}\left(\frac{V\phi_2}{M}\right)+\frac{\partial}{\partial v}\left(\frac{V\phi_1}{M}\right)-\frac{2FM}{V}\phi=0,$$

or $$\frac{2V}{M}\phi_{12}+\phi_2\left(\frac{MV_1-VM_1}{M^2}\right)+\phi_1\left(\frac{MV_2-VM_2}{M^2}\right)-\frac{2FM}{V}\phi=0,$$

or $$\phi_{12}+\tfrac{1}{2}\phi_2\left(\frac{V_1}{V}-\frac{M_1}{M}\right)+\tfrac{1}{2}\phi_1\left(\frac{V_2}{V}-\frac{M_2}{M}\right)-\frac{FM^2}{V^2}\phi=0,$$

or $$\phi_{12}+\Gamma'\phi_1+\Delta'\phi_2+FK\phi=0. \tag{7}$$

Here $\Gamma'$, $\Delta'$, $F$, $K$ are with reference to the surface $S$. If the corresponding quantities for the spherical representation of $S$ be called $\gamma'$, $\delta'$, $f$, $k$, then we know that $\Gamma'=-\gamma'$, $\Delta'=-\delta'$, $FK=f$, and hence we get

$$\phi_{12}-\gamma'\phi_1-\delta'\phi_2+f\phi=0. \tag{8}$$

But $X_{12}=\gamma'X_1+\delta'X_2-fX$, and two similar expressions for $Y_{12}$ and $Z_{12}$.*

$\therefore$ $X$, $Y$, $Z$ are three particular solutions of (8).

Since

$$-\gamma'\equiv\tfrac{1}{2}\frac{\partial}{\partial v}(\log\rho)=\frac{\partial}{\partial v}\log\sqrt{\rho}=\frac{1}{\sqrt{\rho}}\frac{\partial}{\partial v}(\sqrt{\rho})$$

and $$-\delta'\equiv\tfrac{1}{2}\frac{\partial}{\partial u}(\log\rho)=\frac{1}{\sqrt{\rho}}\frac{\partial}{\partial u}(\sqrt{\rho}),‡$$

(8) can be written as

$$\phi_{12}+\frac{\phi_1}{\sqrt{\rho}}\frac{\partial}{\partial v}(\sqrt{\rho})+\frac{\phi_2}{\sqrt{\rho}}\frac{\partial}{\partial u}(\sqrt{\rho})+f\phi=0. \tag{9}$$

Putting $\phi\sqrt{\rho}=\theta$, we get, differentiating with regard to $u$,

$$\phi_1\sqrt{\rho}+\phi\frac{\partial}{\partial u}(\sqrt{\rho})=\theta_1.$$

Differentiating with regard to $v$, we get

$$\phi_{12}\sqrt{\rho}+\phi_1\frac{\partial}{\partial v}(\sqrt{\rho})+\phi_2\frac{\partial}{\partial u}(\sqrt{\rho})+\phi\frac{\partial^2\sqrt{\rho}}{\partial u\partial v}=\theta_{12}.$$

* Forsyth, *Diff. Geom.* p. 261.

‡ Eisenhart, *Diff. Geom.* p. 192.

$$\therefore \quad \phi_{12}+\frac{\phi_1}{\sqrt{\rho}}\frac{\partial}{\partial v}(\sqrt{\rho})+\frac{1}{\sqrt{\rho}}\phi_2\frac{\partial}{\partial u}(\sqrt{\rho})=\frac{1}{\sqrt{\rho}}\theta_{12}-\frac{1}{\sqrt{\rho}}\frac{\partial^2\sqrt{\rho}}{\partial u\partial v}\phi.$$

$$\therefore \text{(9) becomes} \quad \theta_{12}=\left(\frac{1}{\sqrt{\rho}}\frac{\partial^2\sqrt{\rho}}{\partial u\partial v}-f\right)\theta \tag{10}$$

whose three particular solutions $\theta_1$, $\theta_2$, $\theta_3$, say, are given by $\theta_1=X\sqrt{\rho}$, $\theta_2=Y\sqrt{\rho}$, $\theta_3=Z\sqrt{\rho}$.

$\therefore$ $\xi_1$ and $\xi_2$ given by (5) and (6) can be expressed in the forms $\left(\theta_1\frac{\partial\theta}{\partial u}-\theta\frac{\partial\theta_1}{\partial u}\right)$ and $\left(\theta_1\frac{\partial\theta}{\partial v}-\theta\frac{\partial\theta_1}{\partial v}\right)$ respectively.

Similarly $\eta_1$, $\eta_2$, $\zeta_1$, $\zeta_2$ can be expressed in the forms $\left(\theta_2\frac{\partial\theta}{\partial u}-\theta\frac{\partial\theta_2}{\partial u}\right)$, $\left(\theta_2\frac{\partial\theta}{\partial v}-\theta\frac{\partial\theta_2}{\partial v}\right)$, $\left(\theta_3\frac{\partial\theta}{\partial u}-\theta\frac{\partial\theta_3}{\partial u}\right)$, and $\left(\theta_3\frac{\partial\theta}{\partial v}-\theta\frac{\partial\theta_3}{\partial v}\right)$ where $\theta_1$, $\theta_2$, $\theta_3$ are three particular solutions of an equation of the form $\frac{\partial^2\theta}{\partial u\partial v}=\lambda\theta$, and $\theta$ is any other solution.

Hence the surface which corresponds to $S$ with orthogonality of linear elements is given by

$$\left.\begin{aligned}
\xi&=\int\left(\theta_1\frac{\partial\theta}{\partial u}-\theta\frac{\partial\theta_1}{\partial u}\right)du-\left(\theta_1\frac{\partial\theta}{\partial v}-\theta\frac{\partial\theta_1}{\partial v}\right)dv,\\
\eta&=\int\left(\theta_2\frac{\partial\theta}{\partial u}-\theta\frac{\partial\theta_2}{\partial u}\right)du-\left(\theta_2\frac{\partial\theta}{\partial v}-\theta\frac{\partial\theta_2}{\partial v}\right)dv,\\
\zeta&=\int\left(\theta_3\frac{\partial\theta}{\partial u}-\theta\frac{\partial\theta_3}{\partial u}\right)du-\left(\theta_3\frac{\partial\theta}{\partial v}-\theta\frac{\partial\theta_3}{\partial v}\right)dv.^*
\end{aligned}\right\} \tag{III}$$

Now if we choose $\lambda=\frac{2}{(u+v)^2}$, and

$$\theta_1=-\frac{2a}{u+v}+a', \quad \theta_2=-\frac{2b}{u+v}+b', \quad \theta_3=-\frac{2c}{u+v}+c',$$

where $a$, $b$, $c$ are functions of $u$ only, then the surfaces given by (I) are ruled surfaces.†

When these values are substituted, (I) becomes

$$\left.\begin{aligned}
x&=\frac{2(b'c-bc')}{u+v}+\int(b'c''-b''c')du\\
y&=\frac{2(ac'-ca')}{u+v}+\int(c'a''-a'c'')du\\
z&=\frac{2(ba'-ab')}{u+v}+\int(a'b''-b'a'')du
\end{aligned}\right\} \tag{IV}$$

* Cf. Darboux, *loc. cit.* Vol. IV, p. 25.

† See Haag, *loc. cit.* p. 317.

which are the equations of the ruled surface $S$ referred to asymptotic lines as parametric curves.*

Also we know that the general solution of the equation

$$\frac{\partial^2\theta}{\partial u\partial v}=\frac{2}{(u+v)^2}\theta$$

is given by

$$\theta=\frac{2(A+B)}{u+v}-(A'+B')$$

where $A$ is an arbitrary function of $u$ only and $B$ is an arbitrary function of $v$ only.‡

When the values of $\theta$, $\theta_1$, $\theta_2$, $\theta_3$ are substituted in (III) we get

$$\left.\begin{aligned}\xi&=a'B'+\frac{2(aA'-a'A-aB'-a'B)}{u+v}+\int(A'a''-A''a')\,du,\\ \eta&=b'B'+\frac{2(bA'-b'A-bB'-b'B)}{u+v}+\int(A'b''-A''b')\,du,\\ \zeta&=c'B'+\frac{2(cA'-c'A-cB'-c'B)}{u+v}+\int(A'c''-A''c')\,du\end{aligned}\right\}\quad\text{(V)}$$

which are the equations of the surface $S'$ which corresponds to the ruled surface given by (IV) with orthogonality of corresponding elements.

* The equations of a ruled surface referred to asymptotic lines have also been obtained in terms of quadratures by Lelieuvre, *Bull. Sci. Math.* (1888), 126; Villat, *Nouv. Ann. Math.* (1910), 97; and in a form free from quadratures, by Koenigs, *Comptes Rendus* (1888), p. 51.

‡ Darboux, *loc. cit.* Vol. II, p. 143.

# THE ALGEBRA OF THE *eth* POWER RESIDUES

*By* T. VENKATARAYUDU, *Andhra University, Waltair.*

[Received 3 February 1938]

1. *Introduction.* The main object of the present paper is to show that the algebra of the Gaussian periods is identical with the algebra of the *e*th power residues mod $p$ where $p$ is a prime and $e$ is a divisor of $p-1$. This algebra is obviously a particular case of the algebra of the *e*th power residues mod $N$ where $N$ is any integer. Since the system of residue classes mod $N$ is abstractly identical with a cyclic group of order $N$, the above algebra may be interpreted to be the algebra of the *e*th power residues connected with a cyclic group of order $N$. It is therefore natural to enquire whether there is a similar algebra connected with any finite Abelian group. We shall however show by means of an example that this is not the case.

This paper may be regarded as a continuation of a recent paper* by Dr. R. Vaidyanathaswamy *viz.* "The algebra of the quadratic residues", and the notation is the same in both.

2. *The classification of elements in a finite group G.* It is well known that the conjugate classes of elements in a finite group $G$ combine among themselves by the group operation, in the sense that if $C_iC_j$ denotes the totality of the elements obtained by combining every element of the class $C_i$ with every element of the class $C_j$ by the group operation and if an element of the class $C_k$ occurs exactly $\gamma(i, j, k)$ times in $C_iC_j$, then every element of $C_k$ occurs the same number of times $\gamma(i, j, k)$ in $C_iC_j$. The conjugate classes of elements thus determine an algebra which is called by Dr. R. Vaidyanathaswamy the Frobenius algebra. Vaidyanathaswamy showed† that this classification of elements in a finite group is only a particular case of a more general classification of elements in the group such that the classes combine among themselves by the group operation.

THEOREM 1. *If $H$ is any group of automorphisms of $G$ and if an element $S$ of $G$ and all elements which correspond to $S$ by $H$*

* *Jour. Ind. Math. Soc.* 2 (1937), 239.

† *Proc, Ind. Acad. Sc.* 5 (1937), 63.

*are put into a class, the classes so formed combine among themselves by the group operation.*

PROOF: If $S$, an element of a class $B_k$, occurs exactly $t$ times in $B_iB_j$ the element $a(S)$ must occur precisely $t$ times in

$$a(B_iB_j) = a(B_i).a(B_j) = B_i.B_j$$

where $a$ is any automorphism in $H$. By a proper choice of $a$, $a(S)$ can represent any element of the class $B_k$. (Since $H$ is a group, the classes thus formed are exclusive). Hence the truth of the theorem.

When $H$ is the group of inner automorphisms of $G$, the classes of elements of $G$ defined as in the above theorem are the conjugate classes of elements. When $H$ is the total group of automorphisms some of the conjugate classes are grouped together so as to form new classes which again combine among themselves by the group operation.

Vaidyanathaswamy applied the general principle of Theorem 1 to the following two particular cases, and solved the more difficult problem of actually constructing the multiplication table of the classes.

(a) The classification of the residue classes mod $N$ defined by the total group of automorphisms of the additive cyclic group of the residue classes mod $N$.

(b) The classification of the residue classes mod $N$ defined by the sub-group of the group of automorphisms formed by the quadratic residue classes mod $N$.

3. *The algebra of the eth power residues mod N.*

LEMMA. *The totality of the distinct elements obtained by raising every element of a finite Abelian group G to any fixed $d^{th}$ power forms a sub-group G(d) of G.*

PROOF: For any two elements $S_1$, $S_2$ of $G$

$$S_1^d.S_2^d = (S_1S_2)^d.$$

It therefore follows that if $G(d)$ is the set of all the distinct elements in $G$ obtained by raising every element to the $d$th power, the product of any two elements of the set is an element in the set, for every element in the set the inverse element is also in the set, and lastly the identity element is in the set. Hence $G(d)$ is a sub-group of $G$.

*Note.* If $g(d, M)$ is the g. c. d. of $d$ and $M$ where $M$ is the order of the group,

$$G\big(g(d, M)\big) = G(d),$$

for, if $d = d_1 d_2$, where $d_1$ is a divisor of $M$ and $d_2$ is prime to $M$

$$G(d_2) = G.$$

Let $G$ be a cyclic group of order $N$, which we can take without loss of generality as the additive group of the residue classes mod $N$. The automorphisms of $G$ correspond to the multiplication of the residue classes by a number prime to $N$, and the total group $T$ of automorphisms of $G$ is the multiplicative group of the residue classes with respect to the numbers less than $N$ and prime to it. The order of $T$ is therefore $\phi(N)$. A class of elements defined by $T$ consists of all the residue classes mod $N$ with respect to the numbers less than $N$ and have the same *g. c. d.* with $N$.

If now $T(2)$ denotes the group formed by the squares of the elements of $T$ (same notation as in the Lemma), it is clear that $T(2)$ consists of the square residue classes or the quadratic residues mod $N$. The algebra of the classes of elements in $G$ defined by $T(2)$ was called by Vaidyanathaswamy *the algebra of the quadratic residues.* Per contra, if $T(e)$ is the sub-group of $T$ formed by the $e$th powers of the elements of $T$, the algebra of the classes of elements of $G$ defined by $T(e)$ is *the algebra of the* $e^{th}$ *power residues.* In view of the note to Lemma 1, we take, in what follows, $e$ as a divisor of $\phi(N)$.

4. *The algebra of the eth power residues mod p.* In this paragraph let $G$ denote the additive cyclic group of the residue classes mod $p$. If $g$ is a primitive root mod $p$, $T$ is the cyclic group (multiplicative) of order $p-1$ generated by the residue class $g$ mod $p$, i.e. the elements of $T$ are

$$g \bmod p,\ g^2 \bmod p,\ g^3 \bmod p, \ldots, g^{p-1} = 1 \bmod p.$$

Let $e$ be a divisor of $p-1$ and let $ef = p-1$.

$T(e)$ is therefore the multiplicative cyclic group generated by $g^e$ mod $p$, and the elements of $T(e)$ are

$$g^e \bmod p,\ g^{2e} \bmod p, \ldots, g^{(f-1)e} \bmod p,\ g^{fe} = 1 \bmod p.$$

The classes of elements of $G$ defined by $T(e)$ may now be taken as $B_0, C_0, C_1, \ldots, C_{e-1}$ where $B_0$ is the zero residue class and $C_r (r = 0, 1, \ldots, e-1)$ is the class consisting of the residue classes

$$g^r \bmod p,\ g^{r+e} \bmod p, \ldots, g^{r+(f-1)e} \bmod p.$$

This is obvious by taking any element $g^r$ mod $p$ in $G$. The elements in $G$ which correspond to $g^r$ mod $p$ by the automorphisms of $T(e)$ are got by multiplying this element successively with the elements of $T(e)$. We thus obtain the class of elements in $C_r$.

If $C_i \oplus C_j$ denotes the totality of the elements obtained by adding each element of $C_i$ to each element of $C_j$, by our general principle of Theorem 1, each element of $C_k$ occurs the same number of times $\gamma(i, j, k)$ in $C_i \oplus C_j$, i.e.

$$\left.\begin{aligned} C_i \oplus C_j &= \Sigma\gamma(i, j, k)\, C_k + n(i, j) B_0, \\ & \qquad i, j, k = 0, 1, \ldots, e-1 \\ C_i \oplus B_0 &= C_i, \quad i = 0, 1, \ldots, e-1 \\ \text{and} \quad B_0 \oplus B_0 &= B_0 \end{aligned}\right\} \qquad (1)$$

5. *The algebra of the Gaussian periods.* Let $\rho$ be a primitive $p$th root of unity, and as before let $g$ be a primitive root mod $p$ and $ef = p-1$. The functions

$$\eta_0 = \rho + \rho^{g^e} + \rho^{g^{2e}} + \ldots + \rho^{g^{(f-1)e}}$$

$$\eta_1 = \rho^g + \rho^{g^{e+1}} + \rho^{g^{2e+1}} + \ldots \rho^{g^{(f-1)e+1}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\eta_r = \rho^{g^r} + \rho^{g^{e+r}} + \ldots + \rho^{g^{(f-1)e+r}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\eta_e = \rho^{g^{e-1}} + \rho^{g^{2e-1}} + \ldots + \rho^{g^{fe-1}}$$

are known as the $f$-nomial or the Gaussian periods. It is well known* that these periods combine among themselves by multiplication.

The following proof is taken from Dickson's paper†

We have

$$\eta_0\eta_k = \sum_{s=0}^{f-1}\sum_{t=0}^{f-1} \rho^{g^{es}} \cdot \rho^{g^{et+k}}.$$

For a fixed $s$, we may replace $t$ by $t+s$ which ranges with $t$ over a complete set of residues mod $f$.

* Mathews, *Theory of Numbers*; Van der Waerden, *Moderne Algebra*, Vol. 1, p. 162

† L. E. Dickson, (1) Cyclotomy, Higher Congruences and Waring's Problem, *Amer. Jour. Math.* 57 (1935), 391.

$$\therefore \quad \eta_0\eta_k = \sum_{s=0}^{f-1}\sum_{t=0}^{f-1} \rho^{g^{es}}.\rho^{g^{e(s+t)+k}}$$

$$= \sum_{s=0}^{f-1}\sum_{t=0}^{f-1} \rho^{g^{es}(1+g^{te+k})} \qquad (A)$$

First let $et+k \equiv O(p)$. Since $0 \leqslant et+k \leqslant ef-1 \leqslant p-2$,

$$et+k = \tfrac{1}{2}(p-1).$$

If $f$ is even, $k$ is divisible by $e$, hence $k=0$, $t=f/2$. But if $f$ is odd, $k$ is divisible by $e/2$, while $k \neq 0$ since $ef/2$ is not divisible by $e$, hence $k=e/2$, $t=(f-1)/2$. Make the definition

$n_k = 1$ if $f$ is even and $k=0$, or if $f$ is odd and $k=e/2$

$n_k = 0$ in all other cases.

Hence $et+k \equiv O(p)$ holds for exactly $n_k$ values of $t$ and the corresponding part of $(A)$ is $fn_k$.

Secondly, let $et+k$ be prime to $p$, hence $et+k$ is congruent to a power of $g$.

$$1+e^{gt+k} \equiv g^{ez+h} \bmod p \qquad (B)$$

where $0 \leqslant h \leqslant e-1$, $0 \leqslant z \leqslant f-1$, and $h$ (as well as $k$) is fixed; let $(h, k)$ be the number of sets of values of $t$ and $z$ each chosen from $0, 1, \ldots, f-1$ for which $(B)$ holds.

Hence $(h, k)$ is unaltered if we increase (or decrease) either $k$ or $h$ by any muliple of $e$. For fixed values of $t$ and $z$ satisfying $(B)$ the corresponding part of $A$ is

$$\sum_{s=0}^{f-1} \rho^{g^{e(s+z)+h}} = \sum_{s=0}^{f-1} \rho^{g^{es+h}} = \eta_h.$$

This completes the proof of

$$\eta_0\eta_k = \sum_{h=0}^{e-1} (k, h)\,\eta_h + f\,.\,n_k, \quad k = 0, 1, \ldots, e-1$$

Replace $\rho$ by $\rho^{g^m}$. Then

$$\eta_m\eta_{m+k} = \sum_{h=0}^{e-1} (k, h)\,\eta_{m+h} + fn_k.$$

**6.** *The identity of the algebra of the eth power residues mod p and the algebra of the Gaussian periods.* Comparing the

periods $\eta_r$ and the classes $C_r$, we observe that the indices of $\rho$ in the expression for $\eta_r$ are precisely the elements in the class $C_r$. If the $\eta$'s combine among themselves by multiplication, the classes $C_r$ combine among themselves by addition and *vice versa*. Therefore if we take $\xi_0 = 1$, we have immediately

$$\left.\begin{aligned} \eta_i\eta_j &= \Sigma\gamma(i, j, k)\eta_k + n(i, j)\xi_0 \\ &\quad \text{for } i, j, k = 0, 1, \ldots, e-1 \\ \xi_0\eta_i &= \eta_i \text{ for } i = 0, 1, \ldots, e-1 \\ \text{and} \qquad \xi_0^2 &= \xi_0. \end{aligned}\right\} \qquad (2)$$

where $\gamma(i, j, k)$, $n(i, j)$ are the same in (2) and (1). We have therefore established the identity of the two algebras.

It may be noted that the problem of the determination of the constants of multiplication $\gamma(i, j, k)$ in the algebra of the Gaussian periods, still awaits complete solution. In a series of articles Dickson* determined the algebra i.e. the multiplication table $\gamma(i, j, k)$ for the particular cases $e = 8, 9, 12, 18$ and also for the case when $e$ is a prime or double a prime. A less general problem was discussed (this too in particular cases only) by Cayley, Burnside and O. Upadhaya†, namely the determination of the cyclotomic polynomial whose roots are $\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}$.

7. $\gamma(i, j, k)$ *is a multiplicative arithmetic function.* Let $N = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ where the $p$'s are primes. If $n_1$ mod $p_1^{a_1}$, $n_2$ mod $p_2^{a_2}, \ldots, n_r$ mod $p_r^{a_r}$ are a given set of residue classes, the residue class $n$ mod $N$ is uniquely determined by the Chinese Remainder theorem and is such that

$$n = n_k \bmod p_k^{a_k} \quad (k = 1, 2, \ldots, r).$$

If $n$ is prime to $N$, it is clear that $n_k$ is prime to $p_k$ and conversely. Hence if $T$ is the total group of automorphisms of the additive cyclic group $G$ of the residue classes mod $N$ and $T_k$ is the total group of the automorphisms of the additive cyclic group $G_k$ of the residue classes mod $P_k^{a_k}$, $T$ is the direct compound of $T_k$'s in the sense that any element of $T$ is determined uniquely from a set of $r$ elements each one from one of the

* L. E. Dickson. (1) Cyclotomy, Higher Congruences and Waring's Problem, *Amer. Jour. Math.* 57 (1935).

(2) Cyclotomy and trinomial congruences, *Trans. Amer. Math. Soc.* 37 (1935).

(3) Cyclotomy when $e$ is composite, *Trans. Amer. Math. Soc.* 38 (1935)

† Burnside, *Proc. Lond. Math. Soc.*, 14 (1914).

component groups of automorphisms $T_k$ and conversely, and the correspondence is established by the Chinese Remainder Theorem.

Similarly if $n$ is an $e$th power of a residue class mod $N$, $n_k$ is also an $e$th power of a residue class mod $p_k^{a_k}$ for $k=1, 2, \ldots, r$,

for if $$n \equiv t^e \bmod N$$

and $$t \equiv t_k \bmod p_k^{a_k}$$

then $$n_k \equiv t_k^e \bmod p_k^{a_k}.$$

It is now easy to see that $T(e)$ is the direct compound of the groups $T_k(e)$, and a class of elements in $G$ defined by $T(e)$ is the direct compound of the classes of elements in $G_k$, defined by $T_k(e)$. If therefore

$$C_i = C_{1i}C_{2i}\ldots C_{ri}$$
$$C_j = C_{1j}C_{2j}\ldots C_{rj}$$
$$C_k = C_{1k}C_{2k}\ldots C_{rj}$$

are the expressions for $C_i$, $C_j$, $C_k$ as direct compounds of the component classes

$$C_i \oplus C_j = (C_{1i} \oplus C_{1j})(C_{2i} \oplus C_{2j})\ldots(C_{ri} \oplus C_{rj})$$

and therefore $\gamma(i, j, k) = \gamma_1(i, j, k) \cdot \gamma_2(i, j, k) \ldots \gamma_r(i, j, k)$ where $\gamma_t(i, j, k)$ is the number of times the class $C_{tk}$ occurs in $C_{ti} \oplus C_{tj}$.

Thus the function $\gamma(i, j, k)$ is a multiplicative arithmetic function of the single argument $N$.

8. *Relation between the constants $\gamma(i, j, k)$ and the number of solutions of a trinomial congruence mod $p^\theta$.*

Let $G$ denote the additive cyclic group of the residue classes mod $p^\theta$. Let $g$ be a primitive root mod $p^\theta$. The total group $T$ of automorphisms is the multiplicative cyclic group generated by the residue class $g$ mod $p^\theta$ and is of order $\phi(p^\theta)$. If $e$ is a divisor of $\phi(p^\theta)$, $T(e)$ is the multiplicative group generated by $g^e$ mod $p^\theta$ and is of order $\phi(p^\theta)/e$.

The classes of elements in $G$ defined by $T$ will be $K_0, K_1, \ldots, K_{\theta-1}$ where $K_t$ consists of all residue classes with respect to the numbers less than $p^\theta$ and have their g. c. d. with $p^\theta$ as $p^t$. Under the group $T(e)$ of automorphisms these classes $K_t$ will be further divided into equinumerous sub-classes consisting of $\dfrac{\phi(p^{\theta-t})}{g(e, \phi(p^{\theta-t}))}$ elements. [The number of elements in $K_t$ is equal

to the number of elements in $G$ of order $p^{\theta-t}$ and is therefore equal to $\phi(p^{\theta-t})$ ].

A typical class of elements in $G$ defined by $T(e)$ consists of the *distinct* elements in

$$g^r p^t \bmod p^\theta,\ g^{r+c}p^t \bmod p^\theta,\ g^{r+2c}\, p^t \bmod p^\theta, \ldots,$$
$$g^{r+\left(\frac{\phi(p^\theta)}{c}-1\right)c}.p^t \bmod p^\theta$$

which we denote by $C_{rt}$. In the above set each element of $C_{rt}$ is obviously repeated

$$\frac{\phi(p^\theta)g(e,\phi(p^{\theta-t}))}{\phi(p^{\theta-t})} = p^t g\left(e,\phi(p^{\theta-t})\right) \text{ times.}$$

Hence $\gamma_{12}(i, j, k)$, the number of times the class $C_{k_1k_2}$ occurs in $C_{i_1i_2}\oplus C_{j_1j_2}$, is equal to

$$\frac{N}{p^{i_2}\, g(e, \phi(p^{\theta-i_2})) \times p^{j_2} g(e, \phi(p^{\theta-j_2}))}$$

where $N$ is the number of solutions of the congruence

$$ax^e + by^e = c \bmod p^\theta,$$

$a, b, c$ being any fixed elements of the classes $C_{i_1i_2}, C_{j_2j_2}, C_{k_1k_2}$.

9. *The case of the general Abelian group*. It is well known that the necessary and sufficient condition that the group of automorphisms of a finite Abelian group $G$ is Abelian is that $G$ should be cyclic. The group of isomorphisms of a non-cyclic Abelian group is non-Abelian. For a non-Abelian group our lemma in paragraph 3 is not true. However it may be possible that the lemma is true for this particular type of non-Abelian groups, namely, the groups of automorphisms of finite Abelian groups. We shall however show by means of an example that the distinct elements obtained by raising every element of a group of automorphisms of an Abelian group do not form a group.

The group of automorphisms of a finite Abelian group of type $(1, 1, \ldots, 1)$, say $r$ in number, has been known to be the group of all matrices of rank $r$ whose elements are the residue class mod $p$ and whose determinants are $\not\equiv O(p)$ where $p^r$ is the order of the group. Let us now examine the case of the Abelian group $G$

$$P_1^3 = 1,\ P_2^3 = 1,\ P_1P_2 = P_2P_1.$$

The group $T$ of automorphisms of $G$ is the group of matrices

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

129108

where $a, b, c, d$ are $\equiv 0, 1, 2, \bmod 3$ and $ad-bc \not\equiv 0 (3)$. This group is of order 48.

It is easy to verify that the squares of the elements of $T$ do not form a group. For example

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

are square elements of $T$. But

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

is not a square element of $T$. Hence the squares of elements of $T$ do not form a group.

Finally I wish to thank Dr. R. Vaidyanathaswamy for suggesting this problem to me.

600 008

JL
Bm 2,N31
N34:3.2

# The Indian Mathematical Society

*Founded in 1907 for the Advancement of Mathematical Study and Research in India.*


THE COMMITTEE.

**President:**

R. P. PARANJPYE, M.A., D.SC., Vice-Chancellor, Lucknow University.

**Treasurer:**

L. N. SUBRAMANIAM, M.A., Madras Christian College, Madras.

**Librarian:**

R. P. SHINTRE, M.A., Professor of Mathematics, Fergusson College, Poona.

**Secretaries:**

R. VAIDYANATHASWAMY, M.A., D.SC., Reader, University of Madras.

RAM BEHARI, M.A., PH.D., St. Stephen's College, Delhi.

**Members:**

G. S. MAHAJANI, M.A., PH.D., Principal and Prof. of Mathematics, Fergusson College, Poona.

T. K. VENKATARAMAN, M.A., Retired Principal, 16, Kalyanaraman Street, Kumbakonam.

M. V. ARUNACHALA SASTRI, M.A., 266, Maredpalley Lines, Secunderabad (Deccan).

A. NARASINGA RAO, M.A., L.T., Professor, Annamalai University, Annamalainagar.

S. CHOWLA, M.A., PH.D, Professor, Govt. College, Lahore.

P. L. SRIVASTAVA, M.A., D.PHIL., (Oxon.), Reader, Allahabad University, Allahabad.

---

OTHER OFFICERS

**Assistant Secretary:**

S. MAHADEVA IYER, M.A., L.T., Presidency College, Madras.

**Joint Librarian:**

D. D. KOSAMBI, M.A., Fergusson College, Poona.

Head-Quarters: Poona.

# Publications of the Indian Mathematical Society.

1. **The Journal of the Indian Mathematical Society,** Vols. I to XIX are available except for a few numbers which are out of stock. The Journal is published as a quarterly from 1934. Annual Subscription Rs. 6.

2. **The Jubilee Volume of the Society,** issued as Vol. XX of the **Journal**. Bound in stiff calico. Price Rs. 10.

3. **Memoir on Cubic Transformations Associated with a Desmic System,** by DR. R. VAIDYANATHASWAMY, pp. 92. Price Rs. 3.

4. **The Mathematics Student,** a quarterly specially devoted to the needs of students and teachers of Mathematics in Colleges and of young research workers. Published 4 times a year. Annual Subscription Rs. 6.
   Bound volumes of **The Mathematics Student** are available: Vols. I, II, III, and IV at Rs. 6 each.

Subscribers for both the quarterlies, the **Journal** and the **Student,** may obtain both for an Annual Subscription of Rs. 9.

*For Copies apply to:*

**S. Mahadeva Iyer, Esq., M.A., L.T.,**
*Presidency College, Madras.*